



АДМИНИСТРАЦИЯ ПРИМОРСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

11 декабря 2019 года

г. Владивосток

№ 838-па

О внесении изменений в постановление Администрации Приморского края от 19 ноября 2018 года № 538-па «Об утверждении Положения о порядке обеспечения защиты информации в Администрации Приморского края, в органах исполнительной власти Приморского края, в аппарате Губернатора Приморского края и аппарате Администрации Приморского края»

На основании Устава Приморского края Администрация Приморского края

ПОСТАНОВЛЯЕТ:

1. Внести в постановление Администрации Приморского края от 19 ноября 2018 года № 538-па «Об утверждении Положения о порядке обеспечения защиты информации в Администрации Приморского края, в органах исполнительной власти Приморского края, в аппарате Губернатора Приморского края и аппарате Администрации Приморского края» (далее – постановление) следующие изменения:

1.1. Изложить наименование постановления в следующей редакции:

«Об утверждении Положения о порядке обеспечения защиты информации в Администрации Приморского края, в органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях, в аппарате Губернатора Приморского края и аппарате Администрации Приморского края»;

1.2. Изложить пункты 1, 2 постановления в следующей редакции:

«1. Утвердить прилагаемое Положение о порядке обеспечения защиты информации в Администрации Приморского края, в органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях, в аппарате Губернатора Приморского края и аппарате

Администрации Приморского края (далее - Положение).

2. Органам исполнительной власти Приморского края и подведомственным им краевым государственным учреждениям, аппарату Губернатора Приморского края и аппарату Администрации Приморского края осуществлять планирование и реализацию организационно-технических мероприятий по защите информации в соответствии с Положением.»;

1.3. Изложить Положение о порядке обеспечения защиты информации в Администрации Приморского края, в органах исполнительной власти Приморского края, в аппарате Губернатора Приморского края и аппарате Администрации Приморского края, утвержденное постановлением, в новой редакции согласно приложению к настоящему постановлению.

2. Департаменту информационной политики Приморского края обеспечить официальное опубликование настоящего постановления.

Губернатор края –
Глава Администрации
Приморского края



О.Н. Кожемяко

Приложение

к постановлению

Администрации Приморского края
от 11 декабря 2019 года № 838-па

ПОЛОЖЕНИЕ

**о порядке обеспечения защиты информации
в Администрации Приморского края, в органах
исполнительной власти Приморского края
и подведомственных им краевых государственных
учреждениях, в аппарате Губернатора Приморского края
и аппарате Администрации Приморского края**

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет структуру системы защиты информации как составной части Государственной системы защиты информации в Российской Федерации, ее задачи, функции и порядок руководства мероприятиями по технической защите информации в Администрации Приморского края, в органах исполнительной власти Приморского края и подведомственных им краевых государственных учреждениях, в аппарате Губернатора Приморского края и аппарате Администрации Приморского края (далее - государственные органы, учреждения).

1.2. Основными целями системы защиты информации в государственных органах являются:

предотвращение или существенное снижение ущерба безопасности информации, составляющей государственный информационный ресурс, с использованием методов и средств технической защиты информации;

организация и координация работ по защите информации в государственных органах и учреждениях.

1.3. Основными задачами системы защиты информации являются:

проведение в государственных органах и учреждениях единой государственной политики по обеспечению безопасности информации;

обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

методическое и информационное обеспечение работ по защите информации в государственных органах и учреждениях;

исключение или существенное затруднение добывания информации средствами иностранных технических разведок путем предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию с целью ее уничтожения, искажения и блокирования;

учет информационных ресурсов, подлежащих защите;

контроль и анализ состояния защиты информации, а также оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления в государственных органах и учреждениях;

планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности в государственных органах и учреждениях;

организация деятельности структурных подразделений государственных органов и (или) государственных гражданских служащих Приморского края, структурных подразделений учреждений и (или) работников учреждений, ответственных за обеспечение защиты информации в государственном органе, учреждении, совершенствование их организационного и информационно-аналитического обеспечения;

совершенствование и развитие организационно-штатной структуры государственных органов, учреждений и системы подготовки кадров в области защиты информации в государственных органах, учреждениях;

повышение эффективности взаимодействия государственных органов, органов местного самоуправления муниципальных образований Приморского края, организаций и граждан при решении задач по обеспечению

информационной безопасности.

1.4. Основными объектами защиты информации государственных органов, учреждений являются:

информация ограниченного доступа, содержащая сведения, составляющие государственную тайну или служебную информацию конфиденциального характера;

информация, не составляющая государственную тайну, содержащаяся в государственных информационных системах;

персональные данные;

объекты критической информационной инфраструктуры;

технические средства и системы, обрабатывающие информацию ограниченного доступа, содержащую сведения, составляющие государственную тайну или служебную информацию конфиденциального характера;

технические средства и системы, обрабатывающие открытую информацию, размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, содержащая сведения, составляющие государственную тайну или служебную информацию конфиденциального характера;

помещения, предназначенные для ведения переговоров, в ходе которых обсуждаются сведения ограниченного доступа, составляющие государственную тайну или служебную информацию конфиденциального характера;

средства вычислительной техники, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, передачу, обработку и хранение информации, не составляющей государственную тайну, содержащейся в государственных информационных системах и в информационных системах персональных данных.

1.5. Основные организационно-технические мероприятия по защите информации на объектах информатизации государственных органов, учреждений:

организационно-режимное обеспечение защиты информации ограниченного доступа, содержащей сведения, составляющие государственную тайну или служебную информацию конфиденциального характера;

обеспечение физической защиты объектов и средств автоматизации;

обеспечение защиты информации от утечки по техническим каналам при ее обработке и хранении на объектах информатизации;

обеспечение защиты информации от несанкционированного доступа, от компьютерных вирусов в государственных информационных системах и в информационных системах персональных данных;

обеспечение безопасности объектов критической информационной инфраструктуры от компьютерных атак;

организация и проведение контроля состояния защиты информации;

подготовка и обучение государственных гражданских служащих Приморского края, ответственных за обеспечение защиты информации в государственных органах, путём повышения квалификации и (или) профессиональной переподготовки, а также сотрудников учреждений, ответственных за обеспечение защиты информации в учреждениях, в порядке, установленном действующим законодательством.

1.6. Проведение мероприятий и работ с использованием защищаемой информации без принятия необходимых мер по защите информации не допускается.

Руководители государственных органов несут персональную ответственность за обеспечение защиты информации, составляющей государственную тайну или служебную информацию конфиденциального характера, а также информации, содержащейся в государственных информационных системах, в информационных системах персональных данных.

Руководители государственных органов, которым на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной

инфраструктуры, а также руководители государственных органов, подведомственным учреждениям которых на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры, несут персональную ответственность за обеспечение безопасности таких объектов.

Руководители учреждений, которым на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры, несут ответственность за обеспечение безопасности таких объектов в соответствии с действующим законодательством.

II. СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Структуру системы защиты информации государственных органов, учреждений образуют:

Губернатор Приморского края;

вице-губернатор Приморского края, курирующий вопросы записи актов гражданского состояния, гражданской обороны и защиты населения от чрезвычайных ситуаций, защиты государственной тайны, мобилизационной подготовки, военно-патриотического воспитания молодежи;

Совет по информационной безопасности при Губернаторе Приморского края;

Постоянно действующая техническая комиссия по защите государственной тайны при Администрации Приморского края;

экспертная комиссия по проведению экспертизы ценности секретных документов, их отбора для передачи на хранение или для уничтожения;

руководители государственных органов, осуществляющих работу со сведениями, составляющими государственную тайну или служебную информацию конфиденциального характера, обрабатываемыми на специально предназначенных средствах вычислительной техники;

руководители государственных органов, осуществляющих обработку

информации, не составляющей государственную тайну или служебную информацию конфиденциального характера, содержащуюся в государственных информационных системах и в информационных системах персональных данных;

руководители государственных органов, которым на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры;

руководители государственных органов, подведомственным учреждениям которых на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры;

руководители учреждений, которым на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры;

государственные гражданские служащие Приморского края, ответственные за обеспечение защиты информации в государственных органах;

сотрудники учреждений, ответственные за обеспечение защиты информации в учреждении.

III. ПОРЯДОК РУКОВОДСТВА СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ФУНКЦИИ ЕЁ УЧАСТНИКОВ

3.1. Губернатор Приморского края возглавляет систему защиты информации государственных органов.

3.2. Вице-губернатор Приморского края, курирующий вопросы записи актов гражданского состояния, гражданской обороны и защиты населения от чрезвычайных ситуаций, защиты государственной тайны, мобилизационной подготовки, военно-патриотического воспитания молодежи, возглавляет и осуществляет руководство работой Совета по информационной безопасности при Губернаторе Приморского края и Постоянно действующей технической

комиссии по защите государственной тайны при Администрации Приморского края.

3.3. Совет по информационной безопасности при Губернаторе Приморского края является постоянно действующим коллегиальным органом, обеспечивающим координацию деятельности территориальных органов федеральных органов исполнительной власти Приморского края, государственных органов, органов местного самоуправления муниципальных образований Приморского края, организаций по вопросам обеспечения защиты информации.

3.4. Постоянно действующая техническая комиссия по защите государственной тайны при Администрации Приморского края является постоянно действующим коллегиальным органом, обеспечивающим координацию деятельности государственных органов по защите информации ограниченного доступа, содержащей сведения, составляющие государственную тайну или служебную информацию конфиденциального характера, от утечки по техническим каналам и противодействию иностранным техническим разведкам.

3.5. Экспертная комиссия по проведению экспертизы ценности секретных документов, их отбора для передачи на хранение или для уничтожения осуществляет работы по отбору для передачи на постоянное хранение в государственное казенное учреждение «Государственный архив Приморского края» или для уничтожения утративших практическое значение и не имеющих исторической или иной ценности документов и дел с документами, содержащими сведения, составляющие государственную тайну, срок которых истек.

3.6. Руководители государственных органов, осуществляющих работу с информацией, содержащей сведения, составляющие государственную тайну или служебную информацию конфиденциального характера, обрабатываемой на специально предназначенных средствах вычислительной техники, осуществляют организацию и контроль за своевременной реализацией мер

защиты соответствующей информации.

3.7. Руководители государственных органов, учреждений, осуществляющих обработку информации, не составляющей государственную тайну или служебную информацию конфиденциального характера, содержащуюся в государственных информационных системах и в информационных системах персональных данных, осуществляют организацию и контроль за своевременной реализацией мер защиты соответствующей информации.

3.8. Организацию работ по обеспечению безопасности объектов критической информационной инфраструктуры и выполнению требований Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) осуществляют:

руководители государственных органов, которым на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры;

руководители государственных органов, подведомственным учреждениям которых на праве собственности, аренды, праве хозяйственного ведения или оперативного управления принадлежат объекты критической информационной инфраструктуры.

IV. ПЛАНИРОВАНИЕ, РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ

4.1. Структурное подразделение по информационной безопасности органа исполнительной власти Приморского края, обеспечивающего реализацию полномочий в сфере защиты государственной тайны, информации и мобилизационной подготовки Приморского края (далее – отдел информационной безопасности), осуществляет планирование работ по защите информации от иностранных технических разведок и от ее утечки по

техническим каналам в государственных органах, разрабатывая:

планы работы Совета по информационной безопасности при Губернаторе Приморского края;

планы работы Постоянно действующей технической комиссии по защите государственной тайны при Администрации Приморского края;

планы устранения замечаний, выявленных комиссией Управления ФСТЭК России по Дальневосточному федеральному округу в государственных органах;

планы по реализации Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

планы по реализации Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

планы по периодической проверке аттестованных объектов информатизации;

планы основных организационно-технических мероприятий по защите информации в государственных органах;

планы проведения выездных совещаний по вопросам обеспечения информационной безопасности в муниципальных образованиях Приморского края;

планы совместной деятельности Регионального центра мониторинга компьютерных атак Управления Федеральной службы безопасности Российской Федерации по Хабаровскому краю и департамента по защите государственной тайны, информационной безопасности и мобилизационной подготовки Приморского края по обеспечению антивирусной защиты информационных систем и средств вычислительной техники;

планы проверок состояния защиты информации, утверждаемые Губернатором Приморского края.

V. КОНТРОЛЬ ОРГАНИЗАЦИИ И СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Контроль организации и состояния защиты информации в государственных органах, учреждениях осуществляется в целях оценки эффективности принимаемых мер по защите информации, своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, оценки эффективности защиты от иностранных технических разведок.

5.2. Контроль организации и состояния защиты информации в государственных органах, учреждениях заключается в проверке выполнения требований действующего законодательства по вопросам защиты информации, а также в оценке достаточности принимаемых мер по защите информации.

5.3. Основными задачами контроля организации и состояния защиты информации в государственных органах, учреждениях являются:

выявление технических каналов утечки информации на объектах защиты, каналов несанкционированного доступа к информации и специальных воздействий на информацию, анализ и инструментальная оценка возможностей иностранных технических разведок по получению информации;

выявление и анализ нарушений установленных норм и требований по защите информации и принятие оперативных мер по пресечению выявленных нарушений;

разработка рекомендаций по устранению выявленных недостатков в организации и состоянии работ по защите информации;

проверка устранения недостатков, выявленных в результате контроля организации и состояния защиты информации в государственных органах.

5.4. Повседневный контроль состояния защищенности объектов информатизации, на которых осуществляются работы со сведениями, составляющими государственную тайну, проводится отделом информационной безопасности департамента по защите государственной тайны, информационной безопасности и мобилизационной подготовки Приморского

края (далее – департамент по защите государственной тайны Приморского края) в государственных органах ежедневно.

Контроль за эксплуатацией объектов информатизации, на которых осуществляются работы со сведениями, составляющими государственную тайну или служебную информацию конфиденциального характера, проводится отделом информационной безопасности в государственных органах ежемесячно, в соответствии с планом по периодической проверке аттестованных объектов информатизации.

5.5. Контроль эффективности работы средств защиты информации, установленных на объектах информатизации, на которых осуществляются работы со сведениями, составляющими государственную тайну или служебную информацию конфиденциального характера, организуется и проводится отделом информационной безопасности департамента по защите государственной тайны Приморского края в государственных органах раз в два с половиной года, с привлечением специалистов организаций-лицензиатов ФСТЭК России.

5.6. Контроль состояния защиты информации, не составляющей государственную тайну или служебную информацию конфиденциального характера, содержащуюся в государственных информационных системах и в информационных системах персональных данных, организуется и проводится отделом информационной безопасности департамента по защите государственной тайны Приморского края в государственных органах, учреждениях ежегодно, с привлечением специалистов организаций-лицензиатов ФСТЭК России, в соответствии с планами проверок состояния защиты информации, утверждаемыми Губернатором Приморского края.

5.7. Контроль мероприятий по защите объектов критической информационной инфраструктуры проводится отделом информационной безопасности департамента по защите государственной тайны Приморского края в соответствии с решениями Межведомственной комиссии полномочного представителя Президента Российской Федерации в Дальневосточном

федеральном округе по информационной безопасности.

VI. СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. С целью совершенствования организации и состояния системы защиты информации ежегодно проводится подведение итогов работы государственных органов, учреждений за прошедший год на заседаниях Совета по информационной безопасности при Губернаторе Приморского края и на заседаниях Постоянно действующей технической комиссии по защите государственной тайны при Администрации Приморского края.