



Департамент Смоленской области по информационным технологиям

УТВЕРЖДАЮ
Начальник Департамента
Смоленской области по
информационным технологиям

_____ / _____ /

«__» _____ 20__ г.

ДОЛЖНОСТНОЙ РЕГЛАМЕНТ
государственного гражданского служащего Смоленской области,
замещающего должность
ведущего специалиста отдела защиты информации
Департамента Смоленской области по информационным технологиям

1. Общие положения

1.1. Настоящий должностной регламент определяет организацию и порядок осуществления профессиональной служебной деятельности государственного гражданского служащего Смоленской области, замещающего должность ведущего специалиста отдела защиты информации Департамента Смоленской области по информационным технологиям (далее – Департамент).

1.2. В соответствии с реестром государственных должностей Смоленской области, должностей государственной гражданской службы Смоленской области, установленным областным законом «О государственных должностях Смоленской области и о государственной гражданской службе Смоленской области», замещаемая должность отнесена:

1.2.1. К категории «специалисты».

1.2.2. К старшей группе должностей гражданской службы категории «В».

1.3. Область профессиональной служебной деятельности государственного гражданского служащего (далее – гражданский служащий): Управление в сфере информационных технологий, связи, массовых коммуникаций и средств массовой информации.

1.4. Вид профессиональной служебной деятельности государственного гражданского служащего: Регулирование в сфере обеспечения информационной и сетевой безопасности.

1.5. Ведущий специалист отдела защиты информации Департамента (далее – ведущий специалист отдела защиты информации) назначается на должность и освобождается от должности приказом начальника Департамента.

1.6. Ведущий специалист отдела защиты информации непосредственно подчиняется начальнику отдела защиты информации.

2. Квалификационные требования для замещения должности гражданской службы

Для замещения должности ведущего специалиста отдела защиты информации устанавливаются квалификационные требования, включающие базовые и профессионально - функциональные квалификационные требования.

2.1 Базовые квалификационные требования

2.1.1. Гражданский служащий, замещающий должность ведущего специалиста отдела защиты информации, должен иметь высшее образование не ниже уровня бакалавриат.

2.1.2. На должность ведущего специалиста отдела защиты информации назначается лицо, без предъявления требований к стажу государственной гражданской службы или работы по специальности, направлению подготовки.

Гражданский служащий, замещающий должность ведущего специалиста отдела защиты информации, должен обладать следующими базовыми знаниями и умениями:

- 1) Знанием государственного языка Российской Федерации (русского языка);
- 2) Знаниями основ:
 - а) Конституции Российской Федерации;
 - б) Федерального закона от 27 мая 2003 г. № 58-ФЗ «О системе государственной службы Российской Федерации»;
 - в) Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
 - г) Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;
- 3) знаниями и умениями в области информационно-коммуникационных технологий.

2.1.3. Умения гражданского служащего, замещающего должность ведущего специалиста отдела защиты информации, включают следующие умения.

Общие умения:

- умение мыслить системно (стратегически);
- умение планировать, рационально использовать служебное время и достигать результата;
- коммуникативные умения;
- умение управлять изменениями.

Управленческие умения:

- умение эффективно планировать, организовывать работу и контролировать ее выполнение;
- умение оперативно принимать и реализовывать управленческие решения.

2.2 Профессионально-функциональные квалификационные требования

2.2.1. Гражданский служащий, замещающий должность ведущего специалиста отдела защиты информации, должен иметь высшее образование, по направлению подготовки (специальности): «Государственное и муниципальное управление», «Прикладные математика и физика», «Радиофизика»; укрупненные группы направлений подготовки: «Информатика и вычислительная техника», «Компьютерные и информационные науки», «Информационная безопасность», «Электроника, радиотехника и системы связи», «Математика и механика», «Специальные организационно-технические системы», «Правовое обеспечение национальной безопасности», «Информационная безопасность автоматизированных систем» или иному направлению подготовки (специальности), содержащееся в ранее применяемых перечнях специальностей и направлений подготовки, для которых законодательством об образовании Российской Федерации установлено соответствие указанным специальностям и направлениям подготовки.

2.2.2. Гражданский служащий, замещающий должность ведущего специалиста отдела защиты информации, должен обладать следующими профессиональными знаниями в сфере законодательства Российской Федерации:

1. Кодекс Российской Федерации об административных правонарушениях;

2. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
6. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;
7. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
8. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
9. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
10. Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации»;
11. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;
12. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
13. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
14. Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации»;
15. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;
16. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами»;
17. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
18. Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
19. Постановление Правительства РФ от 6 июля 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;

20. Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении и об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

22. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием СКЗИ»;

23. Приказ ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;

24. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

25. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

26. Устава Смоленской области, областных законов, иных областных нормативных правовых актов.

2.2.3. Иные профессиональные знания необходимые для исполнения должностных обязанностей ведущего специалиста отдела защиты информации:

1. Информационных технологий и применения персонального компьютера, составляющих персонального компьютера, включая аппаратное и программное обеспечение, устройство хранения данных;

2. Современных коммуникаций, сетевых приложений, программного обеспечения;

3. Правовых аспектов в сфере предоставления государственных услуг населению и организациям посредством применения ИКТ;

4. Возможностей и особенностей применения современных ИКТ в государственных органах включая использование возможностей межведомственного документооборота, общих вопросов в области обеспечения информационной безопасности, систем взаимодействия с гражданами и организациями, учетных систем, обеспечивающих поддержку выполнения федеральными органами государственной власти основных задач и функций, систем управления государственными и информационными ресурсами, информационно – аналитических систем, обеспечивающих сбор, хранение, обработку, хранение и анализ данных;

5. Методов информационного обеспечения;
6. Понятие защиты информации, противодействие иностранным техническим разведкам;
7. Порядка создания автоматизированных систем в защищенном исполнении;
8. Программно-технических способов и средств обеспечения информационной безопасности;
9. Системы управления электронными архивами, системы информационной безопасности и управления эксплуатацией;
10. Методов и средств получения, обработки и передачи информации;
11. Порядка разработки системы защиты информации информационной системы, обрабатывающей информацию ограниченного доступа;
12. Понятия криптографической защиты информации. Процессы формирования и проверки электронной цифровой подписи;
13. Порядка проведения специальных исследований, тестовых испытаний, процедур сертификации и лицензирования;
14. Правил делового этикета;
15. Правил и норм охраны труда;
16. Порядка работы со служебной информацией.

2.2.4. Гражданский служащий, замещающий должность ведущего специалиста отдела защиты информации, должен обладать следующими профессиональными умениями:

1. Защиты от несанкционированного доступа к информации;
2. Определения потребности в технических средствах защиты;
3. Перевода информации в единый формат;
4. Выполнения работ по обеспечению комплексной защиты информации на основе разработанных программ и методик;
5. Расчетов, анализа и обобщения результатов, составления технических отчетов и оперативных сводок по вопросам защиты информации;
6. Установки сетевого программного обеспечения на серверах и рабочих станциях и поддержки их в рабочем состоянии;
7. Мониторинга сети, выявление ошибок пользователей и сетевого программного обеспечения, восстановление работоспособности системы;
8. Внедрения специализированных программно-технических комплексов, информационно-вычислительных и автоматизированных систем, подготовки нормативно-правовых документов, конкурсной документации, соглашений и договоров;
9. Работы с внутренними и периферийными устройствами компьютера, работы с информационно – телекоммуникационными сетями, в том числе сетью Интернет, работы в операционной системе, управления электронной почтой, работы в текстовом редакторе, работы с электронными таблицами, подготовки презентаций, использования графических объектов в электронных документах, работы с базами данных, работы с системами взаимодействия с гражданами и организациями, работы с системами межведомственного взаимодействия, работы с системами управления государственными информационными ресурсами, работы с информационно –

аналитическими системами, обеспечивающими сбор, обработку, хранение и анализ данных, работы с системами управления электронными архивами, работы с системами информационной безопасности, работы с системами управления эксплуатацией.

3. Должностные обязанности гражданского служащего

Исходя из полномочий, определенных Положением о Департаменте и Положением об отделе защиты информации на ведущего специалиста отдела защиты информации возлагаются следующие обязанности:

3.1. Участвовать в разработке и реализации областных законов и иных нормативных правовых актов, областных программ по развитию информационных технологий и защите информации, а также в реализации на территории Смоленской области в установленном порядке мероприятий федеральных программ и требований федерального законодательства в указанной сфере;

3.2. Участвовать в реализации мероприятий, направленных на обеспечение управления информатизацией Смоленской области, включая разработку стандартов информатизации Смоленской области, нормативно-методических материалов и инструкций в сфере информатизации Смоленской области, осуществление технической защиты информации, использование информационно-коммуникационных технологий, создание типовых решений в сфере региональной информатизации;

3.3. Готовить документацию для реализации функции Департамента в качестве государственного заказчика при размещении заказов на поставки товаров, выполнение работ и оказание услуг в сфере информационных технологий и использования информационно-коммуникационных технологий для государственных нужд, относящихся к сфере деятельности отдела;

3.4. Участвовать в подготовке и проведении конкурсов, выставок, форумов и иных мероприятий в сфере технической защиты информации, использования информационно-коммуникационных технологий и электронной подписи;

3.5. Участвовать в пределах своей компетенции в координации работы по созданию «электронного правительства» Смоленской области, предоставлению государственных услуг через Интернет-портал органов исполнительной власти Смоленской области;

3.6. Участвовать в проведении единой технической политики и осуществлении координации деятельности и методического руководства работами по защите информации в органах исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области;

3.7. Участвовать в осуществлении комплекса мероприятий по защите информации при установлении и осуществлении научно-технических и торгово-экономических связей с зарубежными фирмами, а также при посещении иностранными представителями органов исполнительной власти Смоленской области;

3.8. Осуществлять администрированию средств защиты информации распределенной мультисервисной сети связи и передачи данных органов исполнительной власти и органов местного самоуправления Администрации Смоленской области;

3.9. Проводить мероприятия по защите персональных данных в информационных системах Департамента;

3.10. Участвовать в мониторинге состояния технической защиты информации на территории Смоленской области, по его результатам готовить аналитические и отчетные материалы;

3.11. Участвовать в разработке требований по защите информации при проектировании, строительстве (реконструкции) и эксплуатации объектов информатизации органов исполнительной власти Смоленской области;

3.12. Готовить материалы и участвовать в проведение обучающих семинаров с руководителями и специалистами органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области по вопросам защиты информации;

3.13. Изучать тенденции развития информационных и телекоммуникационных технологий и средств защиты информации;

3.14. Участвовать в ведении Паспорта системы технической защиты информации Смоленской области;

3.15. Участвовать в подготовке отчетов о состоянии работ по защите информации в органах исполнительной власти Смоленской области;

3.16. Готовить предложения по планированию работ по защите от иностранных технических разведок и от ее утечки по техническим каналам в органах исполнительной власти Смоленской области;

3.17. Участвовать в проведении работы по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации в органах исполнительной власти Смоленской области;

3.18. Участвовать в разработке предложений по организации и совершенствованию системы защиты информации в органах исполнительной власти Смоленской области;

3.19. Участвовать в реализации Концепции защиты информации в Смоленской области, решений Комиссии по информационной безопасности при полномочном представителе Президента Российской Федерации в Центральном федеральном округе и Комиссии по информационной безопасности Смоленской области;

3.20. Участвовать в разработке распорядительных и нормативно-методических документов по защите информации в Департаменте;

3.21. Осуществлять внедрение технологий и решений с использованием электронной подписи и обеспечивать их работоспособность

3.22. Готовить ответы на жалобы и обращения граждан, поступающие в Департамент, по вопросам, относящимся к сфере деятельности Отдела.

4. Права гражданского служащего

4.1 На гражданского служащего распространяются основные права, предусмотренные статьей 14 Федерального закона «О государственной гражданской службе Российской Федерации».

4.2 Ведущий специалист отдела защиты информации в пределах своей компетенции имеет право:

4.2.1. Принимать участие в контроле (проверке) органов исполнительной власти Смоленской области за реализацией целевых программ в сфере информационной безопасности.

4.2.2. Участвовать в принятии решений при реализации телекоммуникационных технологий, программных комплексов и прикладных задач пользователей (в сфере защиты информации).

4.2.3. Принимать участие в организации проведения совместно с заинтересованными службами экспертиз телекоммуникационных технологий, банков и баз данных, их централизованной закупке (в сфере защиты информации).

4.2.4. Вносить предложения по совершенствованию работы отдела защиты информации.

5. Ответственность гражданского служащего

Ведущий специалист отдела защиты информации несет ответственность за:

5.1 Неисполнение (ненадлежащее исполнение) возложенных на него должностных обязанностей, а также требований, ограничений и запретов, установленных статьями 15-17 Федерального закона «О государственной гражданской службе Российской Федерации».

5.2 Действие или бездействие, ведущее к нарушению Регламента Администрации Смоленской области, Инструкции по делопроизводству в органах исполнительной власти Смоленской области.

5.3 Разглашение сведений, ставших ему известными в связи с исполнением должностных обязанностей.

5.4 Несоблюдение правил внутреннего трудового распорядка, норм, правил и инструкций по охране труда и пожарной безопасности.

6. Перечень вопросов, по которым гражданский служащий вправе или обязан самостоятельно принимать управленческие и иные решения

В соответствии со своей компетенцией ведущий специалист отдела защиты информации вправе самостоятельно принимать решения по вопросам, перечисленным в разделах 3, 4 настоящего должностного регламента.

7. Перечень вопросов, по которым гражданский служащий вправе или обязан участвовать в подготовке проектов правовых актов и (или) проектов управленческих и иных решений

В соответствии со своей компетенцией ведущий специалист принимает участие в разработке проектов областных законов, правовых актов Губернатора Смоленской области, Администрации Смоленской области, проектов управленческих и иных решений, относящихся к компетенции Департамента и отдела защиты информации.

8. Сроки и процедуры подготовки, рассмотрения проектов управленческих и иных решений, порядок согласования и принятия данных решений

Рассмотрение и подготовка документов, проектов управленческих и иных решений, производится в строгом соответствии с Регламентом Администрации Смоленской области.

9. Порядок служебного взаимодействия гражданского служащего в связи с исполнением им должностных обязанностей с гражданскими служащими того же органа исполнительной власти, гражданскими служащими иных органов государственной власти, другими гражданами, а также с представителями организаций

Поручения и указания ведущий специалист даются начальником отдела защиты информации или лицом, исполняющим его обязанности, в устной или письменной форме по вопросам деятельности Департамента и отдела защиты информации, отнесенным к его компетенции, а также в целях исполнения поручений и указаний начальника Департамента.

Официальная переписка в процессе служебного взаимодействия осуществляется в соответствии с Регламентом Администрации Смоленской области и Инструкцией по делопроизводству в органах исполнительной власти Смоленской области.

Служебное взаимодействие с государственными гражданскими служащими органов исполнительной власти и иных органов государственной власти Смоленской области, другими гражданами и организациями строится в рамках деловых отношений на основе принципов служебного поведения, изложенных в статье 18 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Указе Президента РФ от 12.08.2002 № 885 «Об утверждении общих принципов служебного поведения государственных служащих».

10. Показатели эффективности и результативности профессиональной служебной деятельности гражданского служащего

Основными показателями эффективности и результативности профессиональной служебной деятельности ведущего специалиста отдела защиты информации являются:

– личный вклад в выполнение задач, поставленных перед Администрацией Смоленской области и Департаментом;

– добросовестное, квалифицированное и качественное исполнение должностных обязанностей, своевременность и качество выполняемых заданий, поручений;

– оперативное и качественное исполнение приказов, распоряжений и указаний вышестоящих в порядке подчиненности руководителей и непосредственных руководителей, отданных в пределах их должностных полномочий;

– соблюдение Регламента Администрации Смоленской области;

– соблюдение трудовой дисциплины и порядка работы со служебной документацией.

При оценке деятельности учитываются следующие показатели:

– планирование работы (расстановка приоритетов в работе, порядок в документации);

– выполняемый объем работы (количество завершенной и текущей работы вне зависимости от качества);

– качество выполненной работы (тщательность и аккуратность независимо от количества);

– ответственность (исполнение обязанностей в срок с минимумом контроля);

– самостоятельность (способность выполнять задания без жесткого контроля);

– дисциплина (соблюдение служебного распорядка и сроков выполнения работы).

Начальник отдела защиты информации
Департамента Смоленской области по
информационным технологиям

СОГЛАСОВАНО

Начальник отдела аналитики, кадров,
финансового и материального обеспечения
Департамента Смоленской области по
информационным технологиям

Консультант-юрист отдела организации
предоставления услуг в электронном
виде Департамента Смоленской области
по информационным технологиям

11. Лист ознакомления с должностным регламентом

№ п/п	Фамилия, имя, отчество гражданского служащего	Дата и подпись гражданского служащего после ознакомления с должностным регламентом и получения его копии	Дата и номер приказа о назначении на должность гражданской службы	Дата и номер приказа об освобождении от замещаемой должности гражданской службы
1	2	3	4	5