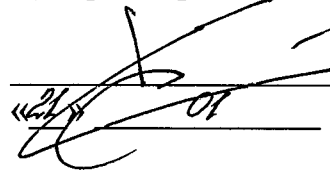


УТВЕРЖДАЮ

Губернатор Свердловской области



Е.В. Куйвашев

2018 год

КОНЦЕПЦИЯ № 01-01-39/2

технической защиты информации на территории Свердловской области

Глава 1. Введение

1. Настоящая концепция представляет собой систему взглядов на проблему технической защиты информации, содержащей сведения, отнесенные к государственной тайне, или сведения, требующие соблюдения конфиденциальности, на территории Свердловской области, а также на цели, задачи, принципы и основные направления формирования и развития системы технической защиты информации на территории Свердловской области (далее – СТЗИ).

2. Настоящая концепция предназначена для использования в Правительстве Свердловской области, исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований, расположенных на территории Свердловской области (далее – муниципальные образования), в подведомственных им организациях.

3. В настоящей концепции используются следующие основные термины и определения:

1) информация – сведения (сообщения, данные) независимо от формы их представления;

2) документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель;

3) информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо;

5) государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

6) конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

7) техническая разведка – деятельность, направленная на добывание разведывательной информации с помощью технических средств;

8) охраняемые от технических средств сведения (охраняемые сведения) – составляющие государственную или служебную тайну сведения об объектах защиты, в отношении которых принято решение об их защите и осуществляется защита от технических разведок;

9) техническая защита информации (далее – ТЗИ) – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с законодательством Российской Федерации, с применением технических, программных и программно-технических средств;

10) объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;

11) объект информатизации – совокупность 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;

12) утечка защищаемой информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

13) технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

14) несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам;

15) информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Глава 2. Общие положения

4. СТЗИ составляет важную составную часть государственной системы ТЗИ на территории Свердловской области.

5. К основным факторам, определяющим необходимость создания и развития СТЗИ, относятся:

1) реструктуризация управления хозяйственной деятельностью, повышение самостоятельности Свердловской области, организаций, находящихся на ее территории;

2) возрастание зависимости результатов деятельности исполнительных органов государственной власти Свердловской области и организаций от достоверности используемой ими информации, своевременности ее получения, надежности принятых мер по сохранению в тайне информации ограниченного доступа;

3) увеличение объемов информации, требующей соблюдения конфиденциальности, циркулирующей в исполнительных органах государственной власти Свердловской области, неоднозначность классификации одной и той же информации при ее обработке в различных государственных и негосударственных учреждениях, необходимость равнопрочной защиты такой информации независимо от места нахождения ее носителей;

4) широкое использование в исполнительных органах государственной власти Свердловской области и подведомственных им организациях региональных и глобальных информационных систем, накапливающих и передающих значительные объемы важной информации и в то же время уязвимых для угроз несанкционированного доступа к информации, требующей соблюдения конфиденциальности, возрастание опасности несанкционированных и непреднамеренных воздействий на информацию в этих системах;

5) возрастание опасности информационных угроз, возникающих в непосредственной близости от защищаемых объектов исполнительных органов государственной власти Свердловской области, подведомственных им организаций или на них самих, использование криминальными структурами устройств негласного получения информации, рост числа преступлений в сфере компьютерной информации, невозможность своевременно и достоверно прогнозировать и выявлять эти угрозы, оценивать их опасность, принимать адекватные меры по их устранению;

6) неспособность большинства организаций, расположенных на территории Свердловской области, самостоятельно обеспечить эффективную защиту информации вследствие отсутствия подготовленных специалистов, необходимой нормативно-методической литературы, высокой стоимости средств ТЗИ и услуг по ее защите;

7) рост числа преступлений в сфере информационных технологий.

6. Основными целями СТЗИ являются:

1) предотвращение или существенное снижение ущерба безопасности Свердловской области, организаций, граждан с использованием методов и средств ТЗИ;

2) обеспечение условий, способствующих реализации государственной политики в сфере информационной безопасности на территории Свердловской области;

3) обеспечению безопасности и устойчивого развития Свердловской области;

4) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

7. Основными задачами СТЗИ являются:

1) проведение единой государственной политики, организация и координация работ по ТЗИ в Свердловской области;

2) исключение или существенное затруднение добывания информации средствами технической разведки, а также предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждение несанкционированного воздействия на информацию с целью ее уничтожения, искажения и блокирования;

3) принятие в пределах своей компетенции правовых актов, регулирующих отношения в области ТЗИ;

4) анализ состояния и прогнозирование источников угроз безопасности информации на территории Свердловской области;

5) формирование и организация деятельности органов по технической защите информации, создание средств ТЗИ и контроля ее эффективности;

6) контроль и анализ состояния ТЗИ в исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований и подведомственных им организациях;

7) выявление ключевых проблем в области ТЗИ, определение направлений развития СТЗИ;

8) научно-техническое, нормативно-методическое и информационное обеспечение работ по ТЗИ в исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований и подведомственных им организациях;

9) совершенствование и развитие системы подготовки специалистов по ТЗИ;

10) обеспечение безопасности информации в системах управления и электронного документооборота в исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований.

8. СТЗИ образуют:

1) Совет по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в Свердловской области;

2) территориальные органы Федеральной службы безопасности Российской Федерации, Министерства внутренних дел Российской Федерации;

3) Правительство Свердловской области;

4) Департамент информатизации и связи Свердловской области, как исполнительный орган государственной власти Свердловской области, ответственный за организацию работ по защите информации, в том числе персональных данных, в Аппарате Губернатора Свердловской области и Правительства Свердловской области, областных и территориальных исполнительных органах государственной власти Свердловской области;

- 5) исполнительные органы государственной власти Свердловской области, постоянно действующие технические комиссии по защите государственной тайны;
 - 6) подразделения (штатные специалисты) исполнительных органов государственной власти Свердловской области;
 - 7) органы местного самоуправления муниципальных образований;
 - 8) подразделения (штатные специалисты) органов местного самоуправления муниципальных образований;
 - 9) организации, подведомственные исполнительным органам государственной власти Свердловской области и проводящие работы с использованием сведений, составляющих государственную тайну, и (или) сведений, требующих соблюдения конфиденциальности;
 - 10) подразделения (штатные специалисты) по ТЗИ организаций, подведомственных исполнительным органам государственной власти Свердловской области;
 - 11) организации, не имеющие ведомственной принадлежности, расположенные на территории Свердловской области и проводящие работы с использованием сведений, составляющих государственную тайну, и (или) сведений, требующих соблюдения конфиденциальности;
 - 12) подразделения (штатные специалисты) по ТЗИ организаций, не имеющих ведомственной принадлежности, расположенных на территории Свердловской области;
 - 13) постоянно действующие технические комиссии по защите государственной тайны исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований, организаций, подведомственных исполнительным органам государственной власти Свердловской области, организаций, не имеющих ведомственной принадлежности, расположенных на территории Свердловской области и проводящих работы с использованием сведений, составляющих государственную тайну, и (или) сведений, требующих соблюдения конфиденциальности;
 - 14) организации, выполняющие работы и оказывающие услуги в области ТЗИ на территории Свердловской области;
 - 15) учебные заведения по подготовке, профессиональной переподготовке и повышению квалификации специалистов в области ТЗИ.
9. К основным объектам защиты в рамках СТЗИ относятся объекты информатизации, объекты органов управления, государственные и муниципальные информационные ресурсы.

Глава 3. Состояние системы технической защиты информации и ключевые проблемы ее развития

10. С 2004 года успешно функционирует Совет по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в Свердловской области (далее – Совет по защите информации).

Одним из важнейших приоритетов в деятельности Совета по защите информации является реализация комплекса мероприятий по обеспечению информационной безопасности в исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований.

В настоящее время решены следующие задачи:

- 1) запущены в эксплуатацию межсетевые экраны;
- 2) организован контроль состояния технической защиты объектов информатизации;
- 3) на всех рабочих станциях установлены лицензионные версии антивирусных программ;
- 4) налажено взаимодействие с Управлением Федеральной службы безопасности Российской Федерации по Свердловской области по вопросам расследования инцидентов в информационной сфере;
- 5) проведены мероприятия по ограничению использования информационных систем и информационно-телекоммуникационных сетей путем установления правил разграничения доступа.

Кроме того, в Свердловской области:

- 1) проводится аттестация автоматизированных рабочих мест;
- 2) проводится аттестация выделенных и защищаемых помещений;
- 3) регулярно актуализируется нормативная правовая база по вопросам работы со сведениями ограниченного распространения, защиты и обработки персональных данных;
- 4) ежегодно для специалистов по ТЗИ исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований проводятся занятия, посвященные требованиям законодательства Российской Федерации в сфере обеспечения безопасности персональных данных при обработке в информационных системах персональных данных.

11. К основным проблемам, характеризующим современное состояние СТЗИ, относятся:

- 1) существенные различия условий развития организационных структур СТЗИ, а также их обеспеченности квалифицированными специалистами, нормативно-методическими документами в области ТЗИ, сертифицированными средствами ТЗИ;
- 2) неравномерное территориальное распределение лицензионных центров, испытательных центров (лабораторий) по сертификации средств ТЗИ, аттестации объектов информатизации по требованиям безопасности информации, подготовке специалистов в области ТЗИ;
- 3) отсутствие современных информационно-аналитических систем поддержки решений в области ТЗИ и обеспечения управления СТЗИ;
- 4) отсутствие оснащения или физический износ средств и аппаратуры контроля эффективности ТЗИ подразделений по защите информации организаций,

подведомственных исполнительным органам государственной власти Свердловской области;

5) низкие темпы формирования необходимой для регламентации и обеспечения деятельности СТЗИ системы нормативных и методических документов в области ТЗИ. Современные информационные технологии для обеспечения потребителей необходимыми документами открытого характера используются слабо.

12. Вследствие существования перечисленных выше проблем обеспечение эффективной ТЗИ в отношении защищаемых объектов становится все более сложной задачей.

13. Одной из приоритетных задач на территории Свердловской области является развитие СТЗИ, что обусловлено необходимостью развития СТЗИ в рамках федеральных целевых программ и государственных программ Свердловской области, а также реализации Концепции технической защиты информации в Уральском федеральном округе.

Глава 4. Цели, принципы и задачи развития системы технической защиты информации

14. Главной целью развития СТЗИ является формирование эффективных компонентов СТЗИ, соответствующих задачам обеспечения национальной безопасности, устойчивого развития Свердловской области.

15. Цели развития СТЗИ заключаются в создании условий, обеспечивающих предотвращение добывания охраняемых сведений об объектах защиты средствами технической разведки в результате предотвращения утечки информации, содержащей сведения, отнесенные к государственной тайне, или сведения, требующие соблюдения конфиденциальности, по техническим каналам, несанкционированного доступа к информации и несанкционированного воздействия на нее в социально-экономической, административно-управленческой, правоохранительной и других сферах деятельности в Свердловской области.

16. Основными принципами развития и деятельности СТЗИ являются:

1) разграничение полномочий федеральных органов исполнительной власти, исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований, подведомственных им организаций по обеспечению ТЗИ;

2) соответствие уровня развития СТЗИ задачам обеспечения национальной безопасности Российской Федерации, безопасности и устойчивого развития Свердловской области с учетом ее экономических возможностей;

3) обеспечение своевременной и адекватной реакции на возникающие на территории Свердловской области и прогнозируемые угрозы ведения технической разведки, утечки информации по техническим каналам, несанкционированного доступа к информации и несанкционированного воздействия на нее;

4) формирование единой технической политики в области защиты информации на территории Свердловской области;

5) сочетание коллегиальности решений, принимаемых в интересах СТЗИ, и полной самостоятельности организаций при выборе средств и способов выполнения этих решений;

6) программно-целевое планирование развития СТЗИ;

7) сочетание правовых, организационных и технических методов защиты информации.

17. Основными задачами развития СТЗИ, обеспечивающими достижение целей развития СТЗИ, являются:

1) формирование и совершенствование организационной структуры СТЗИ, развитие ее научно-технического и кадрового потенциала;

2) создание необходимых и достаточных правовых, организационных, экономических и научно-технических условий на уровне Свердловской области для обеспечения деятельности СТЗИ;

3) обеспечение эффективной ТЗИ на объектах информатизации исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований и организаций, находящихся в их ведении;

4) создание эффективной и гибкой системы управления деятельностью СТЗИ, приспособленной к изменяющимся условиям.

Глава 5. Основные направления развития системы технической защиты информации

18. Основными направлениями развития СТЗИ, обеспечивающими достижение целей и решение основных задач развития этой системы, являются:

1) при решении задачи формирования и совершенствования организационной структуры СТЗИ, развития ее научно-технического и кадрового потенциала:

назначение одного из заместителей руководителя исполнительного органа государственной власти Свердловской области (подведомственной организации) ответственным за организацию и руководство работами по ТЗИ, создание возглавляемого им Совета по защите информации и постоянно действующей технической комиссии по защите государственной тайны;

создание в исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований, подведомственных им организациях подразделений по ТЗИ (назначение штатных специалистов), наделенных полномочиями по контролю за состоянием защиты информации в указанных органах и подведомственных им организациях, подчиненных заместителю руководителя, ответственному за организацию и руководство работами по защите информации;

функциональное подчинение подразделений по ТЗИ исполнительных органов государственной власти Свердловской области, органов местного

самоуправления муниципальных образований, подведомственных им организаций (штатных специалистов) отделу технической защиты информации Департамента информатизации и связи Свердловской области;

создание и развитие в Свердловской области системы подготовки и переподготовки специалистов в области ТЗИ;

2) при решении задачи создания необходимых и достаточных правовых, организационных, экономических и научно-технических условий для обеспечения деятельности СТЗИ:

совершенствование концептуальных и правовых основ деятельности СТЗИ;

организация и обеспечение работ по выявлению и оценке угроз безопасности информации на территории Свердловской области, прогнозированию их развития, разработке типового перечня угроз безопасности информации для Свердловской области и объектов защиты;

обеспечение нормативными правовыми актами и методическими документами по ТЗИ органов СТЗИ, разработка системы организационно-распорядительных и нормативных документов Свердловской области по ТЗИ, конкретизирующих и дополняющих документы федерального уровня применительно к условиям Свердловской области;

оснащение структурных подразделений по ТЗИ, а также объектов информатизации исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований и подведомственных им организаций современными сертифицированными средствами ТЗИ (в том числе средствами контроля эффективности ТЗИ);

3) при решении задачи обеспечения эффективной ТЗИ на объектах защиты исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований и подведомственных им организаций:

разработка и внедрение типовых систем ТЗИ для объектов защиты исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований и подведомственных им организаций;

проведение мероприятий по ТЗИ при организации региональных выставок, конференций, совещаний с участием представителей иностранных государств, при осуществлении международного информационного обмена, в том числе с использованием открытых информационных систем;

использование сертифицированного общего и специального программного обеспечения, сертифицированных средств ТЗИ;

4) при решении задачи создания эффективной и гибкой системы управления деятельностью СТЗИ, приспособленной к изменяющимся условиям обстановки:

совершенствование взаимодействия федеральных органов исполнительной власти и исполнительных органов государственной власти Свердловской области при организации и ведении ТЗИ на территории Свердловской области;

создание системы мониторинга состояния СТЗИ в интересах информационного обеспечения при принятии решений по ТЗИ.

19. Главными приоритетами развития СТЗИ являются:

1) совершенствование концептуальных и правовых основ деятельности СТЗИ;

2) формирование структурных подразделений (назначение штатных специалистов) по защите информации в исполнительных органах государственной власти Свердловской области, органах местного самоуправления муниципальных образований и подведомственных им организациях, оснащение указанных подразделений средствами защиты информации, а также средствами контроля эффективности защиты информации;

3) организация и выполнение работ по выявлению и оценке угроз безопасности информации в Свердловской области, прогнозированию их развития.

Глава 6. Пути реализации настоящей концепции

20. Основные положения настоящей концепции реализуются в результате целенаправленной деятельности исполнительных органов государственной власти Свердловской области, органов местного самоуправления муниципальных образований и подведомственных им организаций путем выполнения общегосударственных и научно-технических программ Свердловской области в области ТЗИ, а также программ информатизации.

Глава 7. Ожидаемые результаты реализации настоящей концепции

21. Реализация настоящей концепции позволит:

1) создать СТЗИ, обеспечивающую выполнение требований нормативных правовых актов Российской Федерации, действующих в области безопасности информации;

2) решить кадровый вопрос и повысить оснащенность органов СТЗИ высокоэффективными средствами защиты информации, а также средствами контроля эффективности ТЗИ;

3) улучшить обеспеченность органов СТЗИ документами в области ТЗИ.

22. В результате реализации основных направлений развития СТЗИ будет создана система, соответствующая задачам обеспечения национальной безопасности, устойчивого развития Свердловской области с учетом ее экономических возможностей и адекватно реагирующая на угрозы безопасности информации в социально-экономической, административно-управленческой, правоохранительной и других сферах деятельности.