Приказ Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@ “Об утверждении Концепции информационной безопасности Федеральной налоговой службы”

В целях реализации статей 14 и 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196) приказываю:

1. Утвердить Концепцию информационной безопасности Федеральной налоговой службы (далее - Концепция) согласно приложению к настоящему приказу.

2. Начальникам (исполняющим обязанности начальника) структурных подразделений центрального аппарата ФНС России, руководителям (исполняющим обязанности руководителя) территориальных органов ФНС России и организаций, находящихся в ведении ФНС России, организовать ознакомление всех работников с Концепцией и обеспечить соблюдение ее требований в практической работе.

3. Признать утратившим силу приказ ФНС России от 29.08.2006 № САЭ-3-27/559@ «Об утверждении концепции».

4. Контроль за исполнением настоящего приказа оставляю за собой. Руководитель Федеральной

налоговой службы М.В. Мишустин

Концепция

информационной безопасности Федеральной налоговой службы

(утв. приказом Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@)

I. Общие положения

1.1. Назначение Концепции

Настоящая Концепция информационной безопасности Федеральной налоговой службы (далее - Концепция) определяет систему взглядов на проблему обеспечения безопасности информации, обрабатываемой в ФНС России, её территориальных органах и подведомственных организациях, а также при осуществлении информационного взаимодействия налоговых органов между собой, с

федеральными органами государственной власти, при оказании государственных услуг юридическим и физическим лицам. Концепция представляет собой систематизированное изложение целей, задач, принципов построения, организационных и технических аспектов обеспечения информационной безопасности (далее - ИБ), устанавливает требования и практические правила управления обеспечением ИБ, базовый уровень и режим защиты информации, обязательный к исполнению налоговыми органами, а также взаимодействующими организациями и налогоплательщиками, пользующимися информационными ресурсами (далее - ИР) ФНС России.

Федеральная налоговая служба (ФНС России) является федеральным органом исполнительной власти и осуществляет свою деятельность непосредственно и через свои территориальные органы во взаимодействии с другими федеральными органами законодательной и исполнительной власти, органами исполнительной власти субъектов Российской Федерации (далее - государственные органы власти), органами местного самоуправления и иными организациями. ФНС России и ее территориальные органы составляют единую централизованную систему налоговых органов.

Главной задачей налоговых органов является контроль за соблюдением законодательства о налогах и сборах, правильностью исчисления, полнотой и своевременностью внесения в бюджетную систему Российской Федерации налогов и сборов, а в случаях, предусмотренных законодательством, - за правильностью исчисления, полнотой и своевременностью внесения в бюджетную систему Российской Федерации других обязательных платежей, а также за производством и оборотом табачной продукции, за соблюдением валютного законодательства Российской Федерации в пределах своей компетенции. В рамках утвержденных Административных регламентов, ФНС России оказывает государственные услуги, в том числе и в электронном виде, и осуществляет электронное информационное взаимодействие с государственными органами власти.

Правила, позволяющие эффективно организовать процесс обеспечения безопасности информации, представляют сложную иерархическую систему инструкций и регламентов, предназначенных для исполнения различными категориями работников ФНС России. Совокупность таких правил формирует Политику безопасности* ФНС России. Концепция является документом Политики ИБ ФНС России, отражающим официально принятую в ФНС России систему взглядов на обеспечение безопасности информации и пути её решения.

Концепция не является техническим проектом системы защиты информации (далее - СиЗИ), а определяет пути достижения требуемого уровня защищенности информации (обеспечения её целостности, доступности и конфиденциальности) при повседневной деятельности налоговых органов и в ходе оказания государственных информационных услуг через создание продуманной, многокаскадной системы обеспечения информационной безопасности (далее - СОИБ). СОИБ должна строиться на основе комплексирования разнообразных организационных и технических мер защиты,

опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и снижения (ликвидацию) ущерба от их воздействия.

Концепция дает возможность выработки стратегической линии, долгосрочных подходов к комплексному решению задач обеспечения ИБ, учитывающих прогнозы развития информационных технологий, появления новых угроз ИБ, тенденций развития методов и средств защиты информации и позволяющих адаптировать СОИБ к любой достаточно сложной и изменчивой ситуации.

Нормативные и организационно-распорядительные документы ФНС России, затрагивающие вопросы ИБ, должны разрабатываться с учетом положений настоящей Концепции и не противоречить им.

1.2. Сфера применения Концепции

Положения Концепции предназначены для использования в практической деятельности должностных лиц, ответственных за создание и использование информационных систем (далее - ИС) ФНС России и развитие телекоммуникационной инфраструктуры, представителей проектных и сервисных организаций, по обеспечению требуемого уровня защищенности ИР ФНС России, а также участников информационного взаимодействия, по соблюдению ими установленных требований безопасности информации.

Положения Концепции могут быть использованы для обеспечения защиты информации, полученной от органов государственной власти и организаций. Дополнительные или взаимно оговоренные сторонами требования по защите не могут ослаблять уровень ИБ ИС ФНС России.

Концепция должна способствовать установлению единой технической политики в сфере обеспечения ИБ и созданию необходимых условий для соответствующих эффективных действий подразделений налоговых органов. Концепция является методологической основой:

при формировании единой политики обеспечения ИБ в ФНС России;

при разработке и совершенствовании документов методического и организационного обеспечения безопасности информации;

при выработке лицами, ответственными за реализацию политики ИБ, взаимосвязанных и согласованных мер защиты организационного и технического характера;

при разработке уполномоченными лицами ФНС России и проектными организациями предложений по созданию и развитию ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России;

при принятии должностными лицами ФНС России управленческих решений по реализации выработанной политики обеспечения ИБ;

при определении ролей и ответственности должностных лиц и работников ФНС России в сфере обеспечения безопасности информации;

при координации деятельности налоговых органов, учреждений и организаций, подведомственных ФНС России, по созданию, развитию и эксплуатации ИС налоговых органов;

при разработке замысла защиты информации в ИС налоговых органов, концепции облика СиЗИ ИС в соответствии с ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

при разработке технических заданий (далее - ТЗ) на создание (модернизацию) объектов информатизации налоговых органов.

Требования по защите информации и проектированию защищённых ИС ФНС России конкретизируются в других документах Политики ИБ ФНС России с указанием комплекса мер и средств, направленных на выявление, предотвращение и противодействие различным угрозам безопасности информации.

1.3. Правовая основа обеспечения ИБ ФНС России

Правовой основой обеспечения ИБ являются положения Конституции Российской Федерации, федеральных законов, указов Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, нормативных правовых актов законодательства Российской

Федерации, нормативных и руководящих документов ФСТЭК России и ФСБ России по вопросам защиты информации.

При реализации функций государственного управления и оказания государственных услуг ФНС России обрабатывается информация, содержащая сведения, составляющие:

государственную тайну;

налоговую тайну;

персональные данные;

коммерческую и банковскую тайны;

служебную тайну ФНС России и других органов государственной власти;

сведения, на основании которых принимаются управленческие решения в системе финансово-кредитной и банковской деятельности, отнесенные к сведениям ключевой системы информационной инфраструктуры;

открытые сведения, подмена, искажение или уничтожение которых может нанести ущерб интересам отдельных граждан, организаций, обществу и государству в целом.

Базовыми законами в области обеспечения ИБ является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», устанавливающие необходимость защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Основу правового обеспечения деятельности ФНС России устанавливает Налоговый кодекс Российской Федерации (далее - НК РФ), вводящий понятие налоговой тайны.

Особое место в правовой основе обеспечения ИБ занимают Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и положения нормативно-методических документов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (далее - КСИИ).

Действующее в настоящее время постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» относит к служебной тайне любую информацию, которая касается деятельности органов государственной власти, ограничение на распространение которой диктуется служебной необходимостью. Должностные лица и работники налоговых органов могут иметь доступ к производственной (коммерческой) тайне налогоплательщиков, поэтому необходимо также руководствоваться Гражданским кодексом Российской Федерации (далее - ГК РФ) и Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

При организации электронного взаимодействия с другими органами государственной власти, а также оказанием государственных услуг налогоплательщикам, наряду с нормативными документами, регламентирующими технические аспекты защиты телекоммуникационной инфраструктуры системы межведомственного электронного взаимодействия (СМЭВ), административными регламентами, необходимо опираться на положения Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», обеспечивающего юридическую значимость электронных документов.

Необходимо так же учитывать, что одним из направлений государственной политики в сфере информатизации является формирование и защита ИР государства, как национального достояния.

В постановлении Правительства Российской Федерации от 25.12.2009 № 1088 «О единой вертикально интегрированной государственной автоматизированной информационной системе «Управление» предусмотрено обеспечение единства методологической основы для всех ИС органов государственной власти, и в частности, стандартов, технологий, форматов и протоколов взаимодействия, обеспечения комплексной безопасности ИР.

1.4. Цели обеспечения безопасности информации в ФНС России

Главной целью обеспечения безопасности информации в ФНС России является предотвращение (минимизация) ущерба субъектам правоотношений в результате противоправных действий с информацией, приводящих к ее разглашению, утрате, утечке, искажению (модификации), уничтожению или незаконному использованию, либо нарушению работы ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России, используемой для информационного обмена и взаимодействия с органами государственной власти и организациями.

Основными целями обеспечения безопасности информации являются:

предотвращение несанкционированного доступа к информации;

предотвращение нарушений прав субъектов при обработке информации;

предупреждение последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации;

недопущение деструктивного информационного воздействия на информацию.

1.5. Основные задачи обеспечения безопасности информации в ФНС России

Основными задачами, вытекающими из целей обеспечения безопасности информации в ФНС России, являются:

совершенствование политики ФНС России в области ИБ при создании и внедрении ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России;

обеспечение соответствия мер и средств защиты информации в ИС налоговых органов положениям нормативных документов по безопасности информации;

совершенствование нормативно-правовой базы обеспечения ИБ, координация деятельности налоговых органов по защите информации;

обеспечение полноты, достоверности и оперативности получения информации налогоплательщиками и органами государственной власти, а также информационной поддержки принятия управленческих решений центральным аппаратом ФНС России;

защита от вмешательства в процесс функционирования ИС налоговых органов посторонних лиц, совершенствование СиЗИ, ее организации, форм и методов предотвращения и нейтрализации угроз ИБ, ликвидации последствий;

предотвращение, в том числе с использованием организационно-правовых мер и технических средств защиты информации, несанкционированных действий и незаконных посягательств на ИР ФНС России со стороны посторонних лиц и работников ФНС России, не имеющих соответствующих полномочий;

регистрация событий, влияющих на безопасность информации, обеспечение полной подконтрольности и подотчетности выполнения всех операций, совершаемых в ИС налоговых органов;

своевременное выявление, оценка и прогнозирование источников угроз, причин и условий, способствующих нанесению ущерба интересам субъектов, нарушению нормального функционирования и развития ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России

анализ рисков реализации угроз, оценка возможного ущерба, предотвращение неприемлемых для ФНС России последствий нарушения ИБ, создание условий для минимизации, локализации и максимально возможного возмещения ущерба;

обеспечение возможности восстановления актуального состояния ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России при нарушении ИБ;

создание системы управления информационной безопасностью.

1.6. Ответственность за реализацию положений Концепции

За реализацию положений Концепции отвечают лица, входящие в организационную структуру системы обеспечения безопасности информации ФНС России, в том числе (но не ограничиваясь):

структурные подразделения центрального аппарата ФНС России;

территориальные органы и подведомственные учреждения ФНС России;

научно-исследовательские организации ФНС России;

разработчики ИС и объектов информатизации ФНС России.

Ответственность за реализацию положений Концепции конкретизируется в должностных регламентах (инструкциях) с учётом организационной структуры ФНС России и локальных нормативных документов ФНС России.

II. Объекты защиты

2.1. Информация, как объект права

ФНС России обеспечивает в пределах своей компетенции защиту сведений, составляющих охраняемую законом тайну, а также контроль и координацию деятельности по защите таких сведений в налоговых органах.

Информация, содержащаяся в ИР ФНС России, а также иные имеющиеся в распоряжении ФНС России сведения и документы являются государственными ИР. Они формируются в процессе деятельности налоговых органов. Часть из них может быть отнесена к общедоступной информации, а часть - к информации ограниченного доступа, в том числе составляющей государственную, налоговую, служебную, коммерческую тайну, персональные данные, информацию о КСИИ или относиться к охраняемым результатам интеллектуальной деятельности. Часть открытых ИР ФНС России содержит сведения, неправомерное обращение с которыми может нанести ущерб гражданам, организациям, обществу.

Осуществление права на ограничение доступа к информации не должно нарушать законные права других лиц на доступ к такой информации. Условия и порядок доступа к ИР определяются обладателем этих ИР.

2.2. Информация, как объект защиты

Объектом защиты являются ИР налоговых органов (библиотеки, архивы и фонды; банки, базы и файлы данных; отдельные документы на традиционных носителях), содержащие зафиксированные на материальном носителе (независимо от его формы) сведения, используемые в процессе сбора, обработки, накопления, хранения, распространения, взаимодействия в рамках исполнения возложенных на ФНС России функций и оказания государственных услуг.

К защищаемым ИР ФНС России относятся:

1. ИР, содержащие информацию ограниченного доступа (распространения):

государственная тайна (в соответствии с «Перечнем сведений, отнесенных к государственной тайне»);

конфиденциальная информация (конфиденциальные ИР), в том числе:

- налоговые ИР;

- ИР персональных данных;

- служебные ИР;

- технологические ИР;

- ИР КСИИ.

Защита ИР, содержащих информацию ограниченного доступа (распространения), представляет собой принятие правовых, организационных и технических мер, направленных на:

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

2) соблюдение конфиденциальности информации;

3) реализацию права на доступ к информации в соответствии с законодательством Российской Федерации;

2. ИР, содержащие общедоступную (публичную) информацию (далее - Открытые ИР).

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не может быть ограничен, а именно к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности налоговых органов, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную тайну или информацию ограниченного доступа (распространения);

4) информации, накапливаемой в государственных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

К Открытым ИР относятся открытые налоговые ИР, открытые регистрационные ИР, общедоступные ИР и инфраструктурные ИР.

Защита Открытых ИР представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от уничтожения, модифицирования, блокирования, а также от иных неправомерных действий в отношении такой информации;

2) реализацию права каждого на доступ к информации.

2.2.1. ИР, содержащие информацию ограниченного доступа (распространения)

К ИР ФНС России, содержащим информацию ограниченного доступа (распространения), относятся государственная тайна и информация конфиденциального характера:

налоговые ИР - ресурсы по государственной регистрации налогоплательщиков; содержащие полученные налоговыми органами сведения о налогоплательщиках: охраняемые налогоплательщиком сведения о производственной деятельности и коммерческой деятельности (ресурсы: «Недействительные паспорта», «Банковские счета», НДС, «Налоговая отчетность по форме 7-НП», «Сведения о физических лицах», частично: «ЕГРИП», «ЕГРЮЛ» в части сведений о номере документа, о дате выдачи и об органе, выдавшем документ, удостоверяющий личность физического лица и т.д.);

ИР персональных данных - ресурсы, содержащие сведения, составляющие персональные данные работников налоговых органов (ресурсы: «Бухгалтерия», «Кадры», «Электронные адреса», «Бюро пропусков», «Учет планирования и распределения путевок работникам ФНС России в ФБЛПУ ФНС России» и другие);

Служебные ИР - ресурсы, содержащие агрегированные сведения, необходимые для обеспечения работы информационно-аналитической системы ФНС России (витрины данных), в том числе

содержащие сведения, необходимые для решения комплексной задачи «Управление финансами», а также содержащие сведения, составляющие служебную тайну взаимодействующих с ФНС России органов государственной власти, передаваемые в рамках межведомственного электронного документооборота (ресурсы: «База данных деклараций об объемах производства и оборота этилового спирта и алкогольной продукции», «Однодневка», «Реестр операций с нефтепродуктами», «Журнал учета федеральных специальных марок для маркировки алкогольной продукции», «СЭД ФНС России», «Финансовое планирование», «Анализ финансово-хозяйственной деятельности налоговых органов» и т.д.);

Технологические ИР - ресурсы, содержащие сведения о принципах, методах, технических решениях и правилах обеспечения безопасности информации в ФНС России и ее территориальных органах (ресурсы: «Безопасность», «Реестр» и т.д.).

2.2.2. Информационные ресурсы, содержащие открытую информацию

К ИР, содержащих открытую информацию, которые подлежат защите от уничтожения, модифицировании, блокирования, а также от иных неправомерных действий в отношении такой информации, и на реализацию права на доступ к информации относятся:

Открытые налоговые ИР - ресурсы, содержащие сведения о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения, а также сведения, передаваемые средствам массовой информации и размещаемые на Интернет-сайтах ФНС России и государственных органов власти, в соответствии с законодательством Российской Федерации;

Базовые государственные ИР - ресурсы, содержащие сведения, по реализации государственной услуги, по регистрации юридических лиц и индивидуальных предпринимателей, а также ресурсы, подключаемые к единой системе межведомственного электронного взаимодействия (ресурсы: «Ответ»; «ЕГРН», «ЕГРИП», «ЕГРЮЛ» (за исключением сведений, отнесенных к информации ограниченного доступа);

Общедоступные ИР - ресурсы, размещаемые на Интернет-сайтах ФНС России и Управлений ФНС по субъектам РФ, на открытых почтовых и публичных серверах ФНС России, содержащие информацию о деятельности налоговых органов в соответствии Федеральным законом № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» (ресурсы: «Правовые БД»; «Жалобы»; «Интернет-сайт ФНС России»; «Интернет-сайты Управлений ФНС по субъектам РФ»). Такие ресурсы могут содержать сведения из реестров, баз данных (за исключением информации ограниченного доступа), электронные издания, архивы,

справочники, словари, тезаурусы, классификаторы, сведения о контрактных и финансово-кредитных отношениях ФНС России с партнерами, статистические сведения, результаты социологических и статистических исследований, открытые аналитические и справочные материалы.

Инфраструктурные ИР - ресурсы, содержащие командную (управляющую и измерительную) и служебно-технологическую информацию (базы и файлы данных, документация, конфигурационные файлы, таблицы маршрутизации, а также информация о подсистемах жизнеобеспечения и физической безопасности, о состоянии каналов связи, планах обеспечения бесперебойной работы) информацию телекоммуникационной инфраструктуры налоговых органов, которая не относится к информации с ограниченным доступом, а также сведения о их создании, структуре, системе управления и защиты.

Нарушение деятельности телекоммуникационной инфраструктуры ФНС России может иметь катастрофические последствия. В таких системах не содержится информации ограниченного доступа, однако, несанкционированное информационное воздействие на системы, осуществляющие сбор, формирование, распространение и использование информации и предназначенные для обеспечения деятельности телекоммуникационной инфраструктуры налоговых органов, может привести к выводу ее из строя или к нарушению ее функционирования.

2.3. Элементы инфраструктуры, как объекты защиты

Информация не может быть рассмотрена в отрыве от элементов инфраструктуры ИС ФНС России (объекта информатизации), на которых она обрабатывается (хранится, обсуждается), поэтому точкой приложения усилий по защите ИР является инфраструктура ИС налоговых органов (объекты информатизации), в том числе:

помещения, здания, объекты, сооружения, передвижные объекты ФНС России, предназначенные для работы с информацией;

оборудование ИС (серверные комплексы, рабочие станции пользователей, технические средства ввода/вывода информации, комплексы сканирования документов, принтеры, средства хранения и архивирования данных, программно-аппаратные средства удостоверяющего центра, источники бесперебойного питания);

телекоммуникационные сети и системы (активное и пассивное коммуникационное оборудование, система управления, мониторинга и обслуживания инфраструктурой);

средства и системы связи и передачи данных (ведомственной, междугородней, городской, внутренней);

программные средства (операционные системы, системы управления базами данных, другое общесистемное, специальное и прикладное программное обеспечение);

средства защиты информации (далее - СЗИ);

технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);

средства обеспечения жизнедеятельности объектов (гарантированные и бесперебойные системы электропитания и заземления объектов, системы пожарной и охранной сигнализации, электронные системы контроля и управления доступом на территорию и в помещения, системы громкоговорящей связи и оповещения, системы кондиционирования, отопления, вентиляции и пожаротушения).

Информация может быть представлена в виде электронных сообщений (электронных документов), формируемых в ходе информационного взаимодействия с государственными органами, исполнения ФНС России своих функций государственного управления и оказания государственных информационных услуг. Используемые при этом технологии информационного взаимодействия должны обеспечивать требуемый уровень защиты ИР при использовании:

обмена электронными сообщениями между налоговыми органами, налогоплательщиками и взаимодействующими структурами;

обмена электронными файлами в рамках электронного документооборота, с применением электронной подписи;

обмена файлами между налоговыми органами и взаимодействующими государственными органами на машинных носителях;

Web-доступа налогоплательщиков при получении государственных услуг с использованием ИР налоговых органов;

технологий терминального доступа работников налоговых органов к ИР ФНС России.

Информация может быть представлена на различных материальных носителях, к которым относятся:

бумажные носители информации (документы);

машинные носители информации (магнитные, магнитооптические, оптические, flash-накопители, карты памяти различных типов и др.);

Информация может распространяться в виде информативных сигналов (электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта информация, обрабатываемая в ИС).

ИС ФНС России относятся к ключевым системам информационной инфраструктуры (КСИИ), которая осуществляет контроль за процессами наполнения бюджета Российская Федерация и официальное информационное обслуживание граждан. В результате деструктивных информационных воздействий на ИС ФНС России может сложиться чрезвычайная ситуация или будут нарушены выполняемые ФНС России функции управления со значительными негативными социальными последствиями.

III. Субъекты отношений

3.1. Российская Федерация, как субъект отношений

В контексте настоящей Концепции, Российская Федерация является субъектом правоотношений в информационной сфере и выступает на равных началах с иными участниками таких отношений. От лица Российской Федерации ее правомочия исполняют органы государственной власти в пределах их компетенции.

Российская Федерация через уполномоченные органы государственной власти осуществляет регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), развитием ИС различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечением взаимодействия таких систем. Российская Федерация может выступать как:

собственник ИР, содержащих сведения, составляющие государственную тайну, независимо от места их расположения;

собственниц государственных ИР, созданных на средства бюджета Российской Федерации;

правообладатель защищаемой авторским правом информации, полученной Российской Федерацией на законных основаниях;

регулятор отношений в информационной сфере и сфере ИБ в Российской Федерации.

3.2. Государственные органы, как субъекты отношений

Управление государственными ИР, осуществляет Правительство Российской Федерации, которое назначает орган государственной власти, наделенный полномочиями реализации от лица государства прав обладателя информации и выступающий самостоятельным субъектом отношений. Компетенция каждого органа государственной власти по владению или пользованию государственными информационными ресурсами устанавливается в Положении о государственном органе, определяющем его статус. Уполномоченные федеральные органы государственной власти выступают так же как организации, осуществляющие реализацию государственной политики в области обеспечения безопасности информации, устанавливающие обязательные и рекомендательные требования по обеспечению защиты информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, а также специальные и контрольные функции.

Органы государственной власти, с которыми ФНС России осуществляет информационное взаимодействие, могут выступать как:

обладатели государственных информационных ресурсов, в том числе, содержащих сведения, составляющие государственную тайну, переданных им в управления в соответствии с их статусом, созданными органами государственной власти для целей исполнения государственных функций и оказания государственных услуг или приобретенными на законных основаниях;

операторы информационных систем, созданных для исполнения им своих государственных функций и предоставления государственных информационных услуг;

операторы персональных данных, организующие сбор и обработку персональных данных, необходимых для исполнения государственных функций и оказания государственных информационных услуг в соответствии с законодательством Российской Федерации и установленными полномочиями;

лица, осуществляющие обработку персональных данных по поручению оператора, которые необходимы им для исполнения государственных функций и оказания государственных информационных услуг;

правообладатели защищаемой авторским правом информации, полученной органом государственной власти на законных основаниях;

пользователи информационных ресурсов ФНС России, необходимых для исполнения государственных функций и оказания государственных услуг;

регуляторы, устанавливающие требования по защите информации, содержащейся в информационных системах и осуществляющие контроль их исполнения, устанавливающие ограничения использования определенных СЗИ и осуществлению отдельных видов деятельности в области защиты информации (только для уполномоченных органов государственной власти).

3.3. Субъекты Российской Федерации, как субъекты отношений

От лица субъекта Российской Федерации субъектом отношений выступают их органы власти и подведомственные им учреждения, наделенные полномочиями, которые в отношениях в информационной сфере могут выступать как:

обладатели ИР, в том числе, содержащих сведения, составляющие государственную тайну, переданных им Российской Федерацией в пределах полномочий по предметам совместного ведения, созданных на средства бюджета субъекта Российской Федерации для целей исполнения установленных функций и оказания государственных услуг или приобретенных на законных основаниях;

операторы ИС, созданных для исполнения им своих государственных функций и предоставления государственных информационных услуг;

операторы персональных данных, организующие сбор и обработку персональных данных, необходимых для исполнения ими своих функций и оказания государственных информационных услуг в соответствии с законодательством Российской Федерации и установленными полномочиями;

лицо, осуществляющее обработку персональных данных по поручению оператора, получившие от ФНС России доступ к персональным данным субъектов, которые необходимы им для исполнения установленных функций и оказания государственных информационных услуг;

правообладатели защищаемой авторским правом информации, полученной органами власти субъекта Российской Федерации и подведомственными им организациями и учреждениями на законных основаниях;

пользователи ИР ФНС России, необходимых им для исполнения своих функций.

3.4. ФНС России, как субъект отношений

ИР ФНС России являются государственными ИР, переданными ей в управление Правительством Российской Федерации от лица Российской Федерации. Компетенция ФНС России по владению и пользованию государственными ИР определена в Положении о Федеральной налоговой службе, устанавливающем ее статус. ФНС России может выступать как:

обладатель государственных ИР, в том числе, содержащих сведения, составляющие государственную тайну, переданных ей в управление в соответствии с установленным статусом, созданных ФНС России для целей исполнения государственных функций и оказания государственных услуг или приобретенных на законных основаниях;

оператор ИС, создаваемых для исполнения ФНС России своих государственных функций и предоставления государственных информационных услуг;

оператор персональных данных, организующий сбор и обработку персональных данных, необходимых для исполнения государственных функций и оказания государственных информационных услуг в соответствии с законодательством Российской Федерации и установленными полномочиями;

лицо, осуществляющее обработку персональных данных по поручению оператора, получившее от других операторов персональных данных доступ к персональным данным, которые необходимы им для исполнения государственных функций и оказания государственных информационных услуг;

правообладатель защищаемой авторским правом информации, полученной ФНС России на законных основаниях;

обладатель ИР, полученных от государственных органов, необходимых для исполнения государственных функций и оказания государственных услуг.

3.5. Государственные учреждения и предприятия, как субъекты отношений

Государственные учреждения и предприятия (далее - госпредприятия) как правило органам государственной власти и их правоотношения в информационной сфере ограничены установленными для них функциями. Установленные требования по защите информации органов государственной власти, являются обязательными для госпредприятий.

Госпредприятия могут осуществлять сбор и обработку информации, в том числе и персональных данных, для целей, установленных законодательством Российской Федерации и (или) необходимых для оказания государственных информационных услуг. Госпредприятия, подведомственные ФНС России, могут выступать как:

обладатели ИР, в том числе, содержащих сведения, составляющие государственную тайну, переданных им ФНС России для целей исполнения ФНС России установленных функций и оказания государственных услуг или приобретенных на законных основаниях;

операторы ИС, созданных для исполнения ФНС России государственных функций и предоставления государственных информационных услуг;

обработчики персональных данных, имеющие поручение от ФНС России на обработку персональных данных субъектов, для исполнения ФНС России установленных функций и оказания государственных информационных услуг;

правообладатели защищаемой авторским правом информации, созданной самими госпредприятиями или по их поручению, а также полученной ими на законных основаниях;

пользователи ИР ФНС России, необходимых для реализации установленных задач.

3.6. Должностные лица и работники, как субъекты отношений

Должностные лица и работники центрального аппарата ФНС России и территориальных налоговых органов, подведомственных госпредприятий, являются субъектами отношений в информационной сфере и могут выступать как:

пользователи ИР ФНС России, необходимых им для исполнения своих должностных обязанностей;

субъекты персональных данных;

правообладатели защищаемой авторским правом информации, созданной самими должностными лицами и работниками или полученной на законных основаниях.

3.7. Юридические и физические лица, как субъекты отношений

Юридические и физические лица являются с одной стороны потребителями государственных информационных услуг, а с другой стороны выступают как источники информации для ИС ФНС России по исполнению ею государственных функций. Юридические лица и индивидуальные предприниматели могут участвовать в разработке и обеспечении функционирования

информационных технологий, автоматизированной поддержки деятельности налоговых органов и предоставлении ФНС России телематических услуг и услуг связи (провайдеры).

Как субъекты отношений в информационной сфере юридические и физические лица могут выступать как:

обладатели, самостоятельно создавшие ИР, необходимые ФНС России для реализации государственных функций или оказания государственных информационных услуг;

субъекты персональных данных (только для физических лиц);

лица, осуществляющие обработку персональных данных по поручению оператора, имеющие поручение от ФНС России на обработку персональных данных субъектов, для исполнения ФНС России установленных функций и оказания государственных информационных услуг;

правообладатели защищаемой авторским правом информации, созданной юридическим или физическим лицами или полученной ими на законных основаниях;

пользователи ИР ФНС России, необходимых им для получения государственных информационных услуг.

IV. Режим защиты информационных ресурсов

4.1. Обобщенная структура информационных ресурсов ФНС России

В ИС налоговых органов могут одновременно использоваться (обрабатываться) ИР различных обладателей информации, по отношению к которым установлены различные требования по степени ограничения доступа (распространения). При этом ИР, отнесенные к одной категории доступа, могут иметь различные степени ограничения доступа.

4.2. Права по установлению требований по защите информационных ресурсов

В зависимости от принадлежности ИР и характера, содержащейся в них информации, ФНС России имеет право установить требования по обеспечению ИБ (режим защиты), или обязана выполнять

требования, установленные уполномоченными органами государственной власти (регуляторами), или другими обладателями информации.

Безопасность информации, содержащей государственную тайну, организуют регуляторы, которые определяют степень защиты и выдвигают требования, обязательные к исполнению всеми организациями на территории Российской Федерации. Такими органами являются:

Межведомственная комиссия (МВК) по защите государственной тайны (в части координации деятельности);

ФСБ России (в части допуска к работам со сведениями, содержащими государственную тайну, и применения криптографических (шифровальных) средств защиты информации);

ФСТЭК России (в части защиты некриптографическими методами).

Требования по защите информации, содержащейся в государственных ИС, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), в пределах их полномочий. При создании и эксплуатации государственных ИС, используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Требования к использованию сети специальной связи и обеспечения ИБ (режим защиты) при использовании системы межведомственного информационного обмена определяются ФСО России.

Требования по защите информации при подключении ИС налоговых органов в рамках взаимодействия к единой системе межведомственного электронного взаимодействия (далее - СМЭВ) определяются соглашением между Минкомсвязи России и ФНС России.

Требования по обеспечению ИБ (режим защиты) открытых (общедоступных) ИР, определяются ФНС России, как их обладателем, самостоятельно на основе требований, определяемых регуляторами, которые в этом случае носят рекомендательный характер. ФНС России, как обладатель сведений на законных основаниях, имеет право предъявлять требования по обеспечению режима защиты,

принадлежащей ей информации, и требовать их соблюдения при передаче такой информации в другие органы государственной власти и третьим лицам. Такие требования носят обязательный характер для всех пользователей.

При обработке персональных данных ФНС России обязана принимать необходимые организационные и технические меры для защиты персональных данных (режим защиты), которые устанавливает Правительство Российская Федерация и регуляторы.

4.3. Порядок установления режима защиты ИР

Режим защиты ИР ФНС России, содержащих государственную тайну, установлен законодательством Российской Федерации.

Режим защиты в отношении ИР ограниченного доступа, не содержащих сведения, отнесенные к государственной тайне, считается установленным после принятия ФНС России следующих мер:

утверждения перечня информации, подлежащей защите в ФНС России;

ограничения доступа к защищаемым ИР, в том числе обращающимся в ИС налоговых органов;

установления порядка обращения с ИР, в том числе другими субъектами;

организации контроля за соблюдением порядка обращения к защищаемым ИР;

организации учета лиц, получивших доступ к защищаемым ИР и (или) лиц, которым защищаемая информация была предоставлена;

урегулирования отношений по использованию защищаемых ИР с работниками (трудовые договоры) и другими субъектами (гражданско-правовые договоры);

нанесения на носители, содержащие защищаемую информацию, соответствующего грифа ограничения доступа (пометки «Для служебного пользования»), если иное не установлено законодательством Российской Федерации.

V. Угрозы безопасности информации и базовая модель нарушителя

5.1. Базовая модель угроз безопасности информации ФНС России

5.1.1. Область применения Базовой модели угроз безопасности информации

Базовая модель угроз содержит единые исходные данные по актуальным для объектов налоговых органов угрозам безопасности информации, связанным с несанкционированным, в том числе случайным, доступом с целью ознакомления, изменения, копирования, неправомерного распространения информации или деструктивных воздействий на элементы ИС и обрабатываемой в них информации. Базовая модель предназначена для формирования обоснованных требований по обеспечению безопасности информации.

Базовая модель угроз представляет собой систематизированный перечень основных актуальных угроз, их источников, уровней реализации угроз, типов материальных объектов среды обработки информации, актуальных для объектов информатизации налоговых органов.

Для отдельных объектов должны быть разработаны Частные модели актуальных угроз, учитывающие особенности обработки информации на конкретном объекте. В качестве методологии выбора актуальных угроз и составления Частных моделей угроз может использоваться общая методология и положения настоящего раздела Концепции.

Базовая модель не применяется для определения требований по защите ИР ФНС России, содержащих государственную тайну, так как требования по защите такой информации устанавливаются регуляторами, исходя из степени секретности обрабатываемой информации, условий расположения ИС и выделенных помещений относительно постоянных представительств иностранных государств, обладающих правом экстерриториальности.

5.1.2. Общий подход к моделированию угроз безопасности информации

Под угрозами безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реальную опасность утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на неё. Систематизация угроз в Базовой модели проведена по виду нарушаемого свойства безопасности информации:

1) угрозы нарушения конфиденциальности:

хищение (утечка, перехват, съем) информации и средств ее обработки;

утрата (неумышленная потеря) информации, средств ее обработки;

разглашение информации;

2) угрозы нарушения целостности информации:

модификация (искажение) информации;

отрицание подлинности информации;

навязывание ложной информации;

3) угрозы нарушения доступности информации:

блокирование информации;

уничтожение информации и средств её обработки и хранения;

Моделирование процессов нарушения безопасности информации осуществляется применительно к объекту информатизации на основе рассмотрения логической цепочки взаимодействия при реализации угрозы:

«угроза - источник угрозы - уровень реализации - уязвимость - последствия».

В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Источники угроз могут находиться как внутри объекта информатизации - внутренние, так и вне его - внешние. Все источники угроз делятся на классы, обусловленные типом носителя угрозы (источника угрозы):

антропогенные источники угроз, обусловленные действиями субъекта, которые могут быть квалифицированы как умышленные или случайные проступки;

техногенные источники угроз, обусловленные техническими средствами и определяемые технократической деятельностью человека;

стихийные источники угроз, обусловленные природными явлениями, которые невозможно предусмотреть или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей.

Угрозы могут быть реализованы только при наличии каких-либо слабых мест - уязвимостей, присущих объекту информатизации и могут быть объективными, субъективными или случайными (Рис. 2 Приложение № 1).

5.1.3. Актуальные источники угроз и уязвимости объектов налоговых органов

Для объектов информатизации налоговых органов основными актуальными источниками угроз безопасности информации для всех или части ИР являются:

иностранные технические разведки (для КСИИ выше 3-го уровня и сведений, содержащих государственную тайну) (антропогенные, внешние);

террористы, криминальные элементы (антропогенные, внешние);

компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе с использованием компьютерных вирусов и других типов вредоносных кодов (антропогенные, внешние);

поставщики программно-технических средств, расходных материалов, услуг, в том числе провайдеры телематических услуг (антропогенные, внешние);

подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования ИС налоговых органов и его ремонт (антропогенные, внешние);

работники налоговых органов, являющиеся легальными участниками процессов обработки информации и действующие вне рамок предоставленных полномочий (антропогенные, внутренние);

работники налоговых органов, являющиеся легальными участниками процессов обработки информации и действующие в рамках предоставленных полномочий (антропогенные, внутренние);

неблагоприятные события природного характера, в том числе пожары, стихийные бедствия, магнитные бури, природные катаклизмы (стихийные);

неблагоприятные события техногенного характера, в том числе аварии на средствах инженерных коммуникаций, средствах телекоммуникационной инфраструктуры, сбои и отказы оборудования (техногенные).

Для объектов налоговых органов актуальными уязвимостями являются:

потенциальная подверженность района размещения объектов налоговых органов воздействию природных и техногенных факторов, в том числе критично близкое расположение техногенных сооружений, географическое положение объекта и климатические условия, гидрологическая и сейсмологическая обстановка, повреждения жизнеобеспечивающих коммуникаций;

ошибки в проектировании объектов информатизации налоговых органов и телекоммуникационной инфраструктуры ФНС России, влияющие на их отказоустойчивость и катастрофоустойчивость, в том

числе сбои электроснабжения, физический износ оборудования и сооружений, малое время наработки на отказ оборудования и ПО;

физические, моральные, психологические особенности работников, создающие предпосылки террористического или криминального воздействия, в том числе: антагонистические отношения (зависть, озлобленность, обида), неудовлетворенность своим положением, неудовлетворенность действиями руководства (взыскание, увольнение), психологическая несовместимость, психические отклонения, стрессовые ситуации, физическое состояние субъекта (усталость, болезненное состояние), психосоматическое состояние субъекта;

недостатки в организации охраны и технической укрепленности объектов налоговых органов, в том числе нарушения режима охраны и защиты (доступа на объект, доступа к техническим средствам), нарушения режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения);

восприимчивость программного обеспечения к вредоносным программным кодам и компьютерным вирусам;

наличие уязвимостей программного и аппаратного обеспечения, в том числе оставление разработчиком (умышленное или случайное) возможностей несанкционированной модификации программного кода, использования среды программирования АИС, программных вызовов;

сбои и отказы технических средств, ошибки при подготовке и использовании программного обеспечения;

наличие уязвимостей (слабостей) СиЗИ;

несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения, некомпетентные действия работников при конфигурировании и управлении программными средствами и оборудованием;

некачественная (неполная) регламентация в договорах (контактах) вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность);

несоответствие регламентов деятельности текущему состоянию объекта защиты и неконтролируемость исполнения работниками ФНС России регламентов своей деятельности, в том числе инсталляции нештатного программного обеспечения, нарушения порядка обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака.

Актуальной считается угроза, которая может быть реализована при обработке информации в ИС налоговых органов и представляет опасность для защищаемой информации. Перечень основных актуальных угроз для объектов налоговых органов приведен в Приложении № 3, а общая классификация методов реализации угроз ИБ в ФНС России приведена в Приложении 4 к настоящей Концепции.

5.2. Базовая модель нарушителя безопасности информации ФНС России

5.2.1. Нарушители безопасности информации ФНС России

Все нарушители делятся на две основные группы: внутренние и внешние.

Под внутренними потенциальными нарушителями подразумеваются работники ФНС России, имеющие санкционированный доступ на территорию налоговых органов или к ИР ФНС России.

Под внешними потенциальными нарушителями подразумеваются все остальные лица.

Перечень потенциальных нарушителей безопасности, который включает внешних и внутренних нарушителей определен регуляторами. В данном разделе рассматриваются особенности, которые могут влиять на ИБ ФНС России.

При организации безопасности информации, содержащей государственную тайну, и на объектах КСИИ 3-й и выше категорий, в качестве потенциальных нарушителей в обязательном порядке должны рассматриваться представители иностранных технических разведок, с точки зрения возможного несанкционированного доступа (НСД) к информации, содержащей государственную тайну, и возможных деструктивных воздействий по техническим каналам на информацию, циркулирующую в КСИИ.

В общем случае разработка системы безопасности информации при обработке сведений, отнесенных к государственной тайне, и/или на объектах КСИИ выше 3-го уровня важности существенно «утяжелит» СиЗИ, как с точки зрения трудозатрат, так и стоимости. Это происходит за счет усиления инженерно-технических мер физической защиты объекта, инженерно-технических мер противодействия техническим каналам утечки или деструктивного воздействия, а так же дополнительных требований по катастрофоустойчивости и надежности.

Рассматриваемые настоящей Концепцией вопросы ИБ в КСИИ ФНС России предусматривают в случае необходимости, возможность создания частных моделей угроз и нарушителя безопасности информации для объектов КСИИ ФНС России.

Применительно к безопасности персональных данных следует руководствоваться Моделью угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных типового объекта информатизации ФНС России.

В соответствии с принципами классификации нарушителей, установленной ФСБ России, и с учетом предположений об имеющихся у них возможностях, нарушители телекоммуникационной инфраструктуры ФНС России относятся к следующим типам: № п/п Вид нарушителя Тип нарушителя

1. Внешние нарушители

1.1 Внешний нарушитель, не имеющий прав доступа в контролируемую зону *

1.2 Сотрудник сторонней организации, не являющийся зарегистрированным пользователем ИС налоговых органов, но имеющий право доступа в контролируемую зону *

2. Внутренние нарушители

2.1 Работник налоговых органов, не являющийся зарегистрированным пользователем ЛВС налогового органа, но имеющий право доступа в контролируемую зону *

Анализ предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности, в соответствии с действующей классификацией, нарушители безопасности телекоммуникационной инфраструктуры ФНС России более всего приближены к типу *. Этот тип нарушителя определяется как внутренний, самостоятельно осуществляющий создание методов и средств реализации атак, а также самостоятельно реализующий атаки. Вместе с тем, при принятии организационных мер защиты,

возможно снижение класса нарушителя до уровня *. Частная модель предполагает необходимость шифрования каналов обмена данными в АИС по классу КС3.

В случае обеспечения безопасности информации при обработке информации, составляющей государственную тайну, требования к СКЗИ могут меняться вплоть до необходимости шифрования информации внутри выделенных сегментов.

При рассмотрении моделей угроз безопасности информации и нарушителя информационной безопасности ФНС России, в данной Концепции не рассматривается возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем АИС, а так же сговора внутреннего и внешнего нарушителей, в связи с применением организационно-технических и кадрово-режимных мер.

При рассмотрении моделей угроз и нарушителя ИБ ФНС России, предполагается, что нарушитель знаком с требованиями безопасности информации (за исключением специальных требований СКЗИ) и является квалифицированным специалистом в области информатизации.

5.3. Возможный ущерб от нарушения безопасности информации

В ходе разработки, внедрения, эксплуатации и совершенствования объектов информатизации налоговых органов, субъектам правоотношений, рассмотренным выше могут быть причинены следующие виды ущерба (вреда):

материальный (экономический) ущерб любому субъекту от разглашения информации, являющейся объектом защиты;

моральный вред, материальный ущерб любому субъекту персональных данных, от их разглашения или нарушения конституционных прав и свобод граждан;

материальный ущерб от необходимости восстановления любым субъектом нарушенных прав и объектов защиты;

моральный вред, материальный ущерб от дезорганизации деятельности ФНС России;

материальный ущерб ФНС России от уничтожения (утраты) объектов защиты;

материальный ущерб, моральный вред от несвоевременного поступления информации потребителям государственных информационных услуг или от нарушения целостности предоставленной информации;

материальный ущерб от невозможности выполнения ФНС России обязательств перед третьей стороной.

Причиненный ущерб может квалифицироваться как состав преступления, предусмотренный уголовным правом, или сопоставляться с рисками утраты, предусмотренными гражданским, административным или арбитражным правом.

Система обеспечения ИБ ФНС России должна обеспечить минимизацию возможного ущерба для субъектов правоотношений, участвующих в информационном обмене и использующих ИР ФНС России.

5.4. Основные методы противодействия угрозам безопасности информации

Вероятность реализации угроз уменьшается различными методами, направленными с одной стороны на устранение носителей угроз - источников угроз, а с другой на устранение или существенное ослабление основ их реализации - уязвимостей. Кроме того, эти методы должны быть направлены на устранение последствий реализации угроз. Среди методов противодействия выделяются следующие основные группы:

правовые методы;

экономические методы;

организационные методы;

инженерно-технические методы;

технические методы;

программно-аппаратные методы.

Выбор совокупного решения по применению нескольких различных групп методов защиты осуществляется с учетом его реализуемости в налоговых органах. Перечень и содержание методов противодействия угрозам приведены в Приложении № 5 к настоящей Концепции.

VI. Организация обеспечения безопасности информации в ФНС России

6.1. Направления сохранения свойств информации для достижения цели обеспечения безопасности информации

6.1.1. Взаимосвязь направлений сохранения свойств информации и угроз ИБ

Главная цель обеспечения ИБ достигается сохранением совокупности свойств информации, к основным из которых относятся:

конфиденциальность защищаемых ИР;

целостность защищаемых ИР;

доступность ИР.

В зависимости от выбранного направления сохранения свойств информации, формируется состав требований к средствам защиты и организационным мероприятиям по ликвидации возможных угроз. Взаимосвязь направлений сохранения свойств информации и угроз безопасности при разработке, модернизации и эксплуатации объектов налоговых органов приведена в Приложении № 1 (Рис. 2).

Направления сохранения свойств информации могут иметь разную степень приоритета для разных ИР ФНС России. Наличие приоритета по одному или нескольким направлениям не исключает

необходимости обеспечения безопасности информации по другим направлениям сохранения свойств информации.

6.1.2. Сводные сведения по приоритетным направлениям сохранения свойств информации

При использовании ИР ФНС России, приоритетными направлениями сохранения свойств информации при обеспечении ИБ являются: Информационные ресурсы ФНС России Приоритеты направлений сохранения свойств информации:

Конфиденциальность	Целостность	Доступность
Конфиденциальные информационные ресурсы ФНС России		
Государственная тайна	Да	Да
КСИИ	Да	
Конфиденциальные налоговые ИР	Да	Да*
ИР персональных данных	Да	Да*
Служебные ИР	Да	Да	Да*
Технологические ИР	Да	
Открытые информационные ресурсы ФНС России		
Базовые государственные ИР	Да	Да
Общедоступные ИР	Да	Да
Коммерческие ИР	Да*	
Инфраструктурные ИР	Да	Да

* Частично.

6.2. Основы построения системы обеспечения безопасности информации ФНС России

6.2.1. Парадигма построения СОБИ ФНС России

Для формирования единой политики обеспечения ИБ ФНС России, достижения требуемого уровня защищенности ИС налоговых органов, оперативного реагирования на возникающие угрозы и негативные тенденции, в ФНС России создается система обеспечения безопасности информации

(далее - СОБИ), как комплекс мер и средств, направленных на выявление, противодействие и ликвидацию различных угроз безопасности информации.

Создание СОБИ направлено на достижение требуемого уровня доверия:

к объектам информатизации налоговых органов, в том числе к телекоммуникационной инфраструктуре ФНС России (территория, помещения, средства обеспечения жизнедеятельности, основные и вспомогательные технические средства и системы);

к субъектам (обладатели информации, субъекты персональных данных, операторы ИС и персональных данных, правообладатели, пользователи, работники налоговых органов, персонал взаимодействующих организаций, вспомогательный персонал, разработчики и поставщики средств обработки информации и программного обеспечения);

к правилам (эксплуатации и технической поддержки объектов информатизации налоговых органов, обслуживания, настройки и ремонта средств обработки информации, пользования и обмена информацией, учета и документирования событий);

к аппаратной (средства обработки информации и вспомогательные технические средства и системы) и программной платформам объектов информатизации налоговых органов (операционные системы, специальное и прикладное программное обеспечение, средства защиты информации, СКЗИ);

к телекоммуникационной инфраструктуре ФНС России (каналообразующая аппаратура, концентраторы и коммутаторы, средства VPN), в том числе выделенным и арендованным каналам связи.

В результате построения СОБИ, вокруг объектов защиты должна быть создана «оболочка», исключающая возможность модификации и любых несанкционированных действий с ними. При построении СОБИ требуется системное согласование средств и способов защиты и создание единой системы управления ИБ (далее - СУИБ). Требуемый уровень безопасности объектов защиты ФНС России достигается:

локализацией ИР ФНС России, требующих защиты;

учетом всех субъектов информационных отношений и всех объектов защиты;

доверенностью конфигурации и настроек программного обеспечения и технических средств ИС налоговых органов;

целостностью всех элементов объектов информатизации налоговых органов и их окружения;

подконтрольностью всех действий с объектами защиты;

документированностью всех событий, влияющих на безопасность информации.

Локализация ИР ФНС России, требующих защиты, достигается разделением ИС налоговых органов на сегменты. При этом, рабочие станции пользователей, имеющих доступ к защищаемой информации одного уровня защищенности, средства отображения, хранения, обработки, ввода, вывода, коммутации и маршрутизации такой информации, равно как и сами ИР, содержащие такую информацию, должны быть обособлены в отдельный сегмент.

Сегменты могут группироваться по степени конфиденциальности, по функциональной потребности, по территориальному размещению средств обработки информации и самих ИР.

Сегментирование может проводиться как на физическом, так и на логическом уровне. Все сегменты сопрягаются между собой только через специальные средства защиты, установленные в точках их сопряжения. Количество точек сопряжения одного сегмента с другими должно быть минимально необходимым (ограниченным). Границей сегмента является внешний по отношению к сегменту порт коммутирующих (маршрутизирующих) устройств или средств защиты, установленных в точке сопряжения с другими сегментами.

Для обеспечения учета субъектов информационных отношений и объектов защиты, все субъекты (рабочие станции пользователей ИС налоговых органов, средства отображения, хранения, обработки, ввода, вывода, коммутации и маршрутизации, прикладные программы и приложения), независимо от степени конфиденциальности и критичности информации, к которым они имеют доступ (возможность обработки), и объекты защиты должны иметь уникальный идентификатор.

Создаваемая СОБИ должна обеспечивать персонификацию любых действий пользователей и администраторов ИС налоговых органов, контролируемый допуск к работе в ИС только зарегистрированных субъектов, прошедших процедуру аутентификации и блокировку работы любого субъекта, не имеющего регистрации.

Всем субъектам должны быть определены роли и полномочия по использованию ИР ФНС России. Любые действия неавторизованными субъектами или субъектами, не имеющими соответствующих полномочий, должны блокироваться. Действия в ИС, не поддающиеся автоматической доверенной регистрации, должны осуществляться по правилу «двух рук», то есть должны выполняться только одновременно несколькими субъектами, предъявляющими соответствующие полномочия.

Доверенность конфигурации и настроек программного обеспечения и технических средств ИС налоговых органов обеспечивается тем, что все элементы ИС налоговых органов, задействованные в обработке защищаемой информации, оборудуются средствами, осуществляющими:

контроль целостности и неизменности программного обеспечения при его загрузке и использовании;

исключение возможности несанкционированной загрузки нештатной операционной системы, прикладных программ или утилит с внешних устройств ввода, в том числе использование командной строки и средств программирования, имеющихся в информационной системе;

авторизацию и разграничение полномочий пользователей;

блокирование несанкционированных процессов обработки защищаемых ИР ФНС России и изменений правил доступа к ним.

Средства обеспечения доверенной загрузки должны обеспечивать контроль целостности общесистемного программного обеспечения, прикладных программ (приложений) и BIOS. Состав контролируемых при загрузке файлов должен определяться в проектной документации на информационную систему.

Целостность элементов объектов информатизации налоговых органов и их окружения достигается применением средств проверки подлинности и неизменности программного обеспечения, а также средств обнаружения и блокирования воздействия вредоносных программ и вирусов. Целостность средств обработки информации и помещений, в которых они размещаются, обеспечивается на физическом уровне.

Подконтрольность действий с объектами защиты и документированность событий, влияющих на безопасность информации, достигается постоянным мониторингом, сбором и накоплением информации о событиях, которые могут повлиять на ИБ, в том числе мониторинг действий пользователей и администраторов ИС налоговых органов, фактов загрузки и инициализации операционных систем, выдачи защищаемой информации на периферийное оборудование, попыток доступа процессов (сервисов) к защищаемым ИР ФНС России или к объектам доступа (рабочие станции пользователей ИС налоговых органов, элементам телекоммуникационной инфраструктуры ФНС России, периферийному оборудованию, томам, каталогам, файлам, записям, полям записей), попытки и факты изменений полномочий субъектов и статуса объектов защиты.

6.2.2. Состав и структура СОБИ

СОБИ не является только технической системой, а объединяет три равнозначные составляющие, имеющие различные объекты воздействия:

организационная база - система организационно-распорядительных документов, определяющих Политику ИБ ФНС России, и персонал, выполняющий установленные правила защиты. Объектом воздействия этой составляющей СОБИ является персонал налоговых органов и взаимодействующих организаций;

исполнительный механизм - совокупность технических, программных и программно-аппаратных средств защиты информации, реализующих, независимо от места их установки, необходимые механизмы защиты. Объектом воздействия этой составляющей СОБИ являются технические, программные и программно-аппаратные средства, непосредственно реализующие механизмы (функции) защиты информации при ее обработке в ИС налоговых органов;

механизм поддержки - комплекс организационных и технических мер противодействия угрозам, осуществляемый различными структурными подразделениями налоговых органов, и обеспечивающий поддержку исполнения установленных правил и реализацию механизмов защиты. Объектом воздействия этой составляющей СОБИ являются организационные меры и вспомогательные средства объектов информатизации налоговых органов.

Содержание основных принципов построения СОБИ, приведено в Приложении № 6 к настоящей Концепции.

В целом, СОБИ ФНС России создается как многоуровневая, иерархическая система, при этом, каждый уровень может иметь несколько слоев. Деление на уровни обусловлено тем, что в пределах каждого уровня выделяются разные группы задач обеспечения ИБ на объектах налоговых органов, решаемые относительно самостоятельно, но при условии использования результатов, достигнутых на остальных уровнях. В составе СОБИ ФНС России выделяются 3 уровня: стратегический, оперативный, исполнительский.

Составляющие СОБИ размещаются на одном или нескольких уровнях. Такое размещение обусловлено тем, что элементы различных составляющих в совокупности могут решать одну группу задач обеспечения ИБ ФНС России (Рис. 3 и 4).

6.2.3. Организационная база СОБИ ФНС России и рекомендации по ее формированию

Организационную базу СОБИ ФНС России составляют работники налоговых органов, которые реализуют и контролируют выполнение установленной в ФНС России Политики обеспечения ИБ, применяя комплекс организационных и инженерно-технических мер противодействия угрозам в совокупности с техническими, программными и программно-аппаратными средствами защиты. В организационную базу СОБИ ФНС России включаются:

работники налоговых органов: должностные лица ФНС России, штатные специалисты отделов информационной безопасности (работники, ответственные за ИБ), информационных технологий и связи налоговых органов (системные администраторы, администраторы операционных систем, баз данных, безопасности информации), а также работники обеспечивающих подразделений (делопроизводства, кадров, жизнеобеспечения и энергоснабжения, физической и пожарной безопасности);

персонал взаимодействующих организаций: сотрудники привлекаемых подразделений физической охраны объектов налоговых органов (МВД России, ФСО России), специалисты операторов связи (провайдеров), сервисных организаций, поставщиков оборудования, а также организаций, разрабатывающих, отлаживающих и сопровождающих прикладное программное обеспечение для нужд ИС налоговых органов;

система организационно-распорядительных документов, определяющих Политику обеспечения ИБ ФНС России: настоящая Концепция, регламенты, положения, инструкции, определяющие роли и ответственность субъектов за обеспечение безопасности информации.

Общее руководство СОБИ ФНС России и принятие всех решений по вопросам ее функционирования осуществляет Руководитель Федеральной налоговой службы.

Подразделения информационной безопасности ФНС России являются ключевыми элементом организационной базы, обеспечивающим подготовку предложений по совершенствованию и реализации положений Политики информационной безопасности ФНС России, осуществляющим взаимодействие с подразделениями налоговых органов и контроль за выполнением установленных требований.

На этапе формирования организационной базы требуется уточнение функциональных обязанностей, прав и полномочий должностных лиц и работников ФНС России в части обеспечения безопасности информации.

Для повышения эффективности защиты информации, целесообразно рассмотреть вопрос введения штатных должностей специалистов по информационной безопасности и администраторов информационной безопасности в налоговых органов.

Администраторы ИС налоговых органов (системные администраторы, администраторы операционных систем, баз данных, безопасности информации) непосредственно реализуют мероприятия по защите ИР, применяют средства защиты, обеспечивают сопровождение объектов защиты, осуществляют контроль за ходом информационных процессов и разграничением доступа к объектам защиты (комплексное администрирование).

Работники налоговых органов, при координирующей роли подразделений ИБ, непосредственно реализуют комплекс организационных и технических мер противодействия угрозам, направленный на достижение требуемого уровня защищенности информации.

Пользователи ИС налоговых органов, независимо от их подчиненности, непосредственно руководствуются положениями Политики ИБ, принятой в ФНС России, соблюдают установленные режимы защиты ИР, обеспечивают строгое исполнение предписанных правил безопасности информации.

Основой для разработки системы организационно-распорядительных документов являются результаты аудита безопасности информации, особенно, в части обследования управления (менеджмента) безопасностью информации.

6.2.4. Исполнительный механизм СОБИ и рекомендации по его построению

Создание исполнительного механизма СОБИ ФНС России осуществляется методом технического проектирования системы защиты информации и системы активной защиты (при необходимости) на основе анализа имеющихся угроз безопасности информации и выбора функций безопасности из числа стандартизированных, а также выполнения рекомендаций стандартов и руководящих документов, позволяющих устранить выявленные уязвимости. При проектировании исполнительного механизма СОБИ, должна быть явно показана устранимость той или иной угрозы (уязвимости) выбранными функциями безопасности.

Исполнительным механизмом СОБИ являются системы защиты информации ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России, в состав которых включаются:

встроенные в общесистемное программное обеспечение ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России функции защиты информации (декларированные функции защиты ОС, СУБД, ПО средств телекоммуникационного и маршрутизирующего оборудования, прикладного ПО);

специальные программные и программно-аппаратные средства защиты, используемые в ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России (средства защиты от НСД к информации, средства повышенной аутентификации, межсетевые экраны, СКЗИ, средства создания доверенных каналов связи, антивирусные средства и т.п.);

средства контроля (мониторинга) состояния ИС налоговых органов, телекоммуникационной инфраструктуры ФНС России и действий пользователей (сканеры сети, сканеры системы, средства контекстного анализа сообщений, средства контроля нежелательной активности пользователей, датчики технических средств охраны, противопожарной сигнализации и т.п.);

средства управления ИБ в ИС налоговых органов и телекоммуникационной инфраструктуре ФНС России (агенты управления, консоли администратора управления, средства регистрации и хранения данных контроля и т.п.).

СиЗИ обеспечивает реализацию практических правил ИБ в ходе процесса обработки защищаемых ИР ФНС России и может эффективно выполнять свои функции только при условии выполнения мер противодействия угрозам, реализуемых механизмом поддержки.

Исполнительный механизм размещается в пределах исполнительского уровня СОБИ и структурируется на 5 подуровней. Задачи исполнительного механизма в пределах каждого подуровня относительно самостоятельны (Рис. 5 Приложение № 1).

Создание исполнительного механизма СОБИ, в основном, сводится к техническому проектированию и построению СиЗИ, соответствующей установленному уровню защищенности ИС налоговых органов, и осуществляется в ходе эскизного и технического проектирования (модернизации) ИС налоговых органов или отдельных их элементов (подсистем, приложений, сегментов).

В ходе проектирования (модернизации) проводится разработка предварительных проектных решений, технико-экономическое обоснование эффективности выбранных вариантов, разработка, монтаж, испытания, сертификация (при необходимости) и тестирование решений и используемых средств защиты информации. При необходимости проводится проектирование помещений с учетом требований нормативных документов по обеспечению ИБ.

6.2.5. Механизм поддержки СОБИ и рекомендации по его построению

Создание механизма поддержки СОБИ осуществляется методом изучения и практического применения существующего передового опыта в области обеспечения безопасности информации, а также выбора необходимых мер защиты из числа рекомендованных, например, изложенных в РД Гостехкомиссия России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», ГОСТ Р ИСО/МЭК 15408-2002 «Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий», международном стандарте ISO/IEC FDIS 27001 «Информационные технологии. Технологии безопасности. Система управления информационной безопасностью. Требования».

Инженерно-технические меры, предусмотренные механизмом поддержки, рассматриваются в ходе проектирования строительства (реконструкции) зданий и помещений налоговых органов. При описании механизма поддержки, должна быть явно показана устранимость той или иной угрозы выбранными организационными и инженерно-техническими мероприятиями.

Механизм поддержки СОБИ составляет комплекс организационных, инженерно-технических и технических мер противодействия угрозам, осуществляемый различными подразделениями налоговых органов, действия которых координируются, управляются и контролируются. В состав механизма поддержки включают:

комплекс организационных мероприятий: система экономического стимулирования, подбора и подготовки работников ФНС России, система физической защиты объектов налоговых органов, разрешительная система допуска персонала, система учета материальных средств, система учета и реагирования на инциденты;

комплекс инженерно-технических мер: система жизнеобеспечения объектов информатизации налоговых органов, системы противопожарной защиты и охранной сигнализации;

комплекс технических мер: системы резервирования каналов связи телекоммуникационной инфраструктуры ФНС России, критического оборудования ИС налоговых органов, система резервного гарантированного и бесперебойного энергоснабжения объектов информатизации налоговых органов.

Механизм поддержки, как и исполнительный механизм, размещается в пределах исполнительного уровня СОБИ и структурируется на 5 подуровней. Однако, содержание задач механизма поддержки, при схожести решаемых задач с задачами исполнительного механизма, различается по формам (способам) реализации (Рис. 6 Приложение № 1).

Состав организационных мероприятий определяется в организационно-распорядительной документации ФНС России, а также исполнительной документацией по вопросам обеспечения ИБ, составляющей третий уровень Политики безопасности (должностные положения и инструкции, эксплуатационные документы СЗИ, таблицы разграничения прав доступа к ИР).

К моменту создания СОБИ на объектах налоговых органов, как правило, уже имеются развернутые и действующие системы пожарной и охранной сигнализаций, а также организована охрана помещений и прилегающих территорий. При создании СОБИ необходимо учитывать, что часть угроз могут быть минимизированы уже имеющимися на объектах налоговых органов техническими средствами и системами.

6.2.6. Система управления информационной безопасностью

Для координации и контроля действий налоговых органов по реализации политики ИБ, в составе СОБИ, на основе соответствующих подразделений налоговых органов, формируется система управления ИБ (далее - СУИБ), построение которой выполнено в соответствии с Концепцией построения системы управления информационной безопасностью ФНС России. Принципы управления представлены в Приложении № 1 (Рис. 8).

Основу СУИБ составляет организационная база СОБИ, которая обеспечивает единую вертикаль управления всеми механизмами СОБИ из единого центра (принцип иерархичности управления) на всех жизненных циклах создания, передачи, обработки и хранения объектов защиты и эксплуатации ИС налоговых органов (принцип непрерывности управления).

Иерархичность СОБИ предполагает создание в ФНС России, вертикальной структуры СУИБ, обеспечивающей проведение единого замысла обеспечения безопасности объектов защиты и автоматизированное документирование всех событий, влияющих на обеспечение ИБ ФНС России с возможностью их последующего анализа (принцип доказательности). Для этого создается отдельная (структурно и физически) административная база данных СУИБ (принцип выделенности).

СУИБ является глубоко интегрированной в элементы СОБИ системой и не может рассматриваться в отрыве от них. СУИБ, являясь составной частью СОБИ, повторяет структуру основной системы - СОБИ (Рис. 9 Приложение № 1). Данная Концепция определяет Политики информационной безопасности СУИБ.

СУИБ, как правило, должна комплектоваться специалистами, имеющими практический опыт работы в области защиты информации и отвечающими соответствующим квалификационным требованиям для специалистов по комплексной защите информации. Их численность должна быть достаточна для обеспечения ИБ. Зачисление работников на временную работу не допускается.

6.3. Архитектура системы обеспечения информационной безопасности ФНС России

6.3.1. Архитектура организационной базы СОБИ ФНС России

Организационная база СОБИ ФНС России строится как иерархически-матричная структура. Иерархичность предполагает создание в ФНС России многоуровневой вертикальной структуры, позволяющей своевременно довести управляющее воздействие до исполнительных механизмов СОБИ и получить оперативную информацию о реакции на эти воздействия для последующего их анализа и коррекции. Матричность предполагает создание разветвленной горизонтальной структуры взаимодействия с подразделениями налоговых органов.

Организационная база архитектурно имеет две составляющие: «Персонал» и «Политика». Первая составляющая определяется и напрямую зависит от организационно-штатной структуры ФНС России, а вторая определяется пакетом организационно-распорядительных документов, направленных на формирование и реализацию Политики безопасности ФНС России.

Элементы организационной базы размещаются на 3 уровнях СОБИ. Общая архитектура организационной базы по уровням СОБИ и их взаимосвязь представлена в Приложении № 1 (Рис. № 10).

Подразделения ИБ налоговых органов являются ядром составляющей «Персонал» организационной базы СОБИ и подчиняются непосредственно руководителю налогового органа. Обязанности, права и полномочия работников подразделений ИБ ФНС России определяются должностными регламентами. При администрировании безопасности информации в ИС налоговых органов должно обеспечиваться сопряжение функций администрирования безопасности информации с функциями системы администрирования процесса обработки информации (комплексное администрирование). Системные администраторы, администраторы операционных систем, администраторы баз данных ИС налоговых органов (подчиненные структурным подразделениям информатизации налоговых органов) непосредственно реализуют мероприятия по защите ИР ФНС России, осуществляют контроль за ходом информационных процессов, обеспечением разграничения доступа к ИР ФНС России в процессе их использования.

Администраторы безопасности информации взаимодействуют со всеми администраторами ИС, обеспечивающими формирование и сопровождение защищаемых ИР ФНС России и контроль за информационными процессами. Задачами администраторов безопасности информации являются:

формирование и контроль списка пользователей ИС налоговых органов, допущенных к работе с каждым видом ИР;

формирование параметров входа в ИС налоговых органов (идентификатора) и ключевых данных пользователей;

контроль текущего состояния ИС налоговых органов, просмотр журнала активных сеансов, контроль за работой конкретных рабочих станций (АРМ) и конкретных пользователей ИС налоговых органов;

контроль за действиями администраторов ИС налоговых органов (администраторов ИС, операционных систем, баз данных) по администрированию штатных (встроенных) для общесистемного программного обеспечения механизмов защиты;

администрирование специализированных средств защиты информации и анализа защищенности ресурсов ИС налоговых органов, поддержка функционирования средств, технологий и процессов обеспечения ИБ ФНС России;

учет наступления системных событий, связанных с инициализацией функций ИС налоговых органов, изменением их конфигурации, а также изменением прав доступа пользователей и процессов.

Численность администраторов безопасности информации и специалистов по защите информации определяется масштабом ИС налоговых органов и объемом защищаемых ИР ФНС России.

Для реализации задач обеспечения безопасности информации, в зависимости от организационно-штатной структуры ФНС России, подразделения налоговых органов в составе СОБИ наделяются следующими полномочиями (но не ограничиваясь):

управлять планами обеспечения ИБ ФНС России;

разрабатывать и вносить предложения по изменению Политики ИБ ФНС России;

изменять существующие и принимать новые организационно-распорядительные и нормативно-методические документы по обеспечению ИБ в ФНС России;

выбирать средства управления и обеспечения ИБ при эксплуатации ИС налоговых органов;

контролировать действия пользователей ИС налоговых органов, в том числе пользователей, имеющих максимальные полномочия;

контролировать активность пользователей ИС налоговых органов, связанную с доступом к ИР ФНС России и использованием средств защиты информации;

осуществлять мониторинг событий ИБ;

расследовать нарушения ИБ и, в случае необходимости, выходить с предложениями по применению санкций в отношении лиц, осуществивших противоправные действия;

участвовать в действиях по восстановлению работоспособности ИС налоговых органов после сбоев и аварий;

создавать, поддерживать и совершенствовать СУИБ ФНС России.

Конкретные полномочия подразделений налоговых органов, в том числе обеспечивающих подразделений (информатизации, делопроизводства, кадров, жизнеобеспечения и энергоснабжения, физической безопасности), по исполнению функций защиты информации определяются в организационно-распорядительном документе «Регламент обеспечения информационной безопасности ФНС России».

Совершенствование и развитие составляющей «Персонал» организационной базы СОБИ ФНС России должно быть направлено на:

создание в центральном аппарате ФНС России и территориальных налоговых органах аппарата администраторов ИБ;

увеличение штата работников подразделений ИБ центрального аппарата ФНС России и территориальных налоговых органов;

оснащение подразделений ИБ программными и программно-техническими средствами мониторинга и контроля состояния ИБ в налоговых органах;

повышение квалификации и профессионализма работников ФНС России, непосредственно задействованных в решении вопросов обеспечения ИБ.

Подготовка и переподготовка пользователей и специалистов ФНС России по защите информации требует создания системы повышения уровня технической грамотности и информированности в области ИБ, а также переподготовки специалистов по защите информации. Для этого необходимо регулярно проводить тренинги для персонала и контроль готовности новых работников по применению правил информационной защиты, а также периодически осуществлять переподготовку специалистов подразделений защиты информации. Особенно важно проводить тренинги при изменении конфигурации ИС налоговых органов (внедрении новых технологий и прикладных систем, смены оборудования, ключевых приложений, новых правил и инструкций).

Политика ИБ ФНС России является собирательным понятием, предполагающим создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, как единых для всех участников информационного обмена (Общая политика), так и специализированных, для территориальных органов и подведомственных учреждений ФНС России (Частная политика), и устанавливающих порядок обеспечения безопасности информации при осуществлении информационного обмена, управления и контроля ИБ, а также выдвигающих требования по поддержанию этого порядка.

Политика ИБ ФНС России направлена на:

нормативное урегулирование процесса обмена защищаемой информации между участниками информационного обмена;

установление организационно-правового режима использования ИР ФНС России, ответственность должностных лиц и работников ФНС России за соблюдение этого режима;

реализацию комплекса организационных, программных и аппаратно-программных мероприятий по обеспечению целостности, доступности и в необходимых случаях конфиденциальности защищаемой информации;

предоставление участникам информационного обмена необходимых сведений для сознательного поддержания установленного уровня защищенности информации;

организацию в ФНС России постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения ИБ;

создание в ФНС России и ее территориальных органах резервов и возможностей по ликвидации последствий нарушения режима защиты информации и восстановления ИБ.

Дополнительно, документы, формирующие Частные политики территориальных налоговых органов, должны определять:

роли и ответственность работников налоговых органов за обеспечение ИБ;

требования по соблюдению конфиденциальности;

порядок классификации ИР;

процедуры управления ИР налоговых органов в соответствии с установленными правилами разграничения доступа;

меры по поддержанию требуемого порядка допуска работников налоговых органов к операциям с ИР;

порядок организации физической защиты объектов информатизации налоговых органов;

порядок проведения регламентных работ и сервисного обслуживания на оборудовании ИС налоговых органов;

порядок реагирования на инциденты и другие вопросы, необходимые для обеспечения требуемого уровня безопасности ИР ФНС России.

Укрупненная структура Политики ИБ ФНС России и краткое содержание входящих в неё основных документов приведена в Приложении № 1 (Рис. 11).

На стратегическом уровне Политики ИБ ФНС России формулируются цели обеспечения безопасности информации, которые в дальнейшем определяют правила и требования по всем вопросам безопасности информации и становятся обязательными для всех участников информационного взаимодействия.

Все последующие технические решения по развитию ИС и телекоммуникационной инфраструктуры ФНС России и защите ИР, должны опираться на выводы данной Концепции.

Оперативный уровень Политики ИБ объединяет единые для ФНС России и частные для каждого налогового органа и учреждения ФНС России организационно-распорядительные документы, регламентирующие вопросы организации и проведения работ по защите информации, положений об инфраструктурных элементах системы обеспечения безопасности информации, разрешительной системе доступа исполнителей к документам и сведениям, регламентах выполнения защищенных информационных процессов, а также технические требования к составляющим элементам СиЗИ. Такими документами являются:

стандарты (Технические требования) по обеспечению ИБ в налоговых органах;

регламенты обеспечения ИБ в налоговых органах.

Регламенты являются документами, отражающими организационную составляющую процесса обеспечения безопасности информации. На основании положений Концепции разрабатывается Регламент обеспечения ИБ ФНС России, который основываясь на описании ИР, используемых при исполнении функций государственного управления и оказания государственных услуг, и требуемого уровня их безопасности, определяет общие правила разграничения доступа к ИР, основные обязанности и ответственность конкретных субъектов отношений за обеспечение безопасности информации, с учетом сложившегося делового стиля общения при исполнении государственных функций управления и оказании государственных информационных услуг.

Регламент обеспечения ИБ ФНС России устанавливает:

правила обеспечения режима защиты конкретных ИР;

правила регистрации пользователей и назначения им прав доступа;

правила работы пользователей с защищаемыми ИР;

порядок контроля режима защиты информации и реагирования на нарушения режима защиты (разбор инцидентов);

порядок ликвидации последствий при возникновении нештатных ситуаций и нарушении установленного режима защиты.

Исполнительский уровень Политики ИБ ФНС России объединяет исполнительную документацию, включающую должностные регламенты и инструкции, а также эксплуатационные документы средств защиты информации (далее - СЗИ), обеспечивающих разграничение доступа к защищаемым ИР, средств мониторинга и контроля. Документы этого уровня основываются на эксплуатационной документации СЗИ и программных компонент.

6.3.2. Архитектура исполнительного механизма СОБИ ФНС России

Исполнительный механизм СОБИ является вспомогательной подсистемой ИС. В отличие от главной целевой функции ИС налоговых органов является - обработка (сбор, накопление, преобразование, хранение) и доставка информации пользователям, СОБИ непосредственно не участвует в процессе обработки информации и ее целевая функция состоит в обеспечении исполнения и контроля установленных правил доступа к ИР ФНС России, то есть в регулировании отношений между субъектами и защищаемыми ИР. Общая архитектура исполнительного механизма СОБИ должна формироваться на основе объединения механизмов защиты различных элементов ИС налоговых органов в функциональные контуры, реализующие те или иные функции безопасности, а не на основе основных процессов обработки информации (Рис. 12 Приложение № 1). Общая архитектура исполнительного механизма СОБИ может не повторять архитектуру ИС налоговых органов.

Исполнительный механизм, непосредственно не влияя на информацию в процессе ее обработки, реализует свои функции через механизмы защиты элементов инфраструктуры и глубоко интегрирован в элементы ИС налоговых органов.

Исполнительный механизм СОБИ ФНС России строится как матричная структура, позволяющая обеспечить надежные горизонтальные связи взаимодействия между отдельными СЗИ, встроенными функциями безопасности общесистемного и прикладного ПО, а также с элементами системы активной защиты (при необходимости). При этом должно обеспечиваться централизованное управление всеми процессами защиты информации.

Роль исполнительного механизма СОБИ исполняет СиЗИ, которая строится как территориально распределенная централизованная автоматизированная система, которая может быть структурирована по следующим функциям:

контур поддержки доверенной среды (ПДС);

контур идентификации и аутентификации субъектов (ИАС);

контур контроля и управления доступом субъектов (КДС);

контур защиты потоков информации (ЗПИ);

контур регистрации и аудита событий (РАС);

контур управления информационной безопасностью (УИБ).

Контур ПДС предназначен для поддержания целостной программно-аппаратной среды ИС налоговых органов и обеспечения гарантий доверительности пользователей при использовании предоставляемых сервисов и оказании государственных услуг. В состав контура ПДС также входят средства защиты от вредоносных программ и вирусов (антивирусные средства), которые охватывают два подуровня: пользовательский и сетевой.

Контур ИАС предназначен для проведения процедур аутентификации/идентификации субъектов доступа, пользующихся ИС налоговых органов на всех этапах обработки и обращения в ней информации. Контур ИАС должен обеспечивать поддержку процесса идентификации (аутентификации) пользователей ИС налоговых органов в случае использования субъектами доступа в качестве средств идентификации (аутентификации) цифровых сертификатов, а также в случае использования в ИС налоговых органов при межведомственном информационном обмене средств подтверждения (проверки) подлинности электронных документов (электронных подписей).

В состав контура ИАС входит Удостоверяющий центр, имеющий в своем составе Центр сертификации (хранилище и центр выдачи сертификатов), Центры регистрации, рабочие станции (АРМ) администраторов Центров регистрации, являющиеся точками регистрации пользователей ИС налоговых органов. УЦ предназначен для обеспечения юридически значимого защищенного электронного документооборота между налоговыми органами и взаимодействия с другими органами государственной власти, а также для формирования идентификаторов (цифровых сертификатов) пользователей ИС налоговых органов.

Контур КДС предназначен для управления и контроля за доступом пользователей ИС налоговых органов к объектам защиты, АРМ, серверам, а также к прикладным системам и сервисам при исполнении им государственных функций и оказании государственных услуг.

Контур ЗПИ предназначен для создания доверенных каналов связи между структурными элементами ИС налоговых органов, а также между ИС налоговых органов и другими взаимодействующими ИС.

Контур РАС предназначен для оперативного оповещения специального подразделения и уполномоченных сотрудников (администраторы безопасности) ФНС России, отвечающих за обеспечение ИБ о состоянии (изменениях) ПО и технических средств обработки информации, используемых в ИС налоговых органов, действиях администраторов и пользователей по конфигурированию ПО и технических средств обработки информации.

Контур УИБ предназначен для оперативного управления отдельными контурами СОБИ и обеспечением безопасности информации в целом на основе установленных правил (политики) ИБ. Входящие в состав контуров элементы должны реализовывать функции безопасности, предусмотренные техническими требованиями Политики ИБ ФНС России или аналогичными требованиями в объеме, необходимом для обеспечения требуемого уровня защищенности ИС налоговых органов.

Функции, которые должны быть реализованы каждым функциональным контуром исполнительного механизма СОБИ для достижения поставленной цели ИБ ФНС России, приведены в Приложении № 7 к настоящей Концепции.

Используемые в СиЗИ средства защиты информации должны пройти оценку соответствия, подтверждающую выполнение ими специальных функций по защите, в соответствии с требуемым классом защищенности, а также (в зависимости от установленного класса защищенности) отсутствие недекларированных возможностей (для программных и программно-аппаратных средств).

Архитектура СиЗИ не должна накладывать жестких ограничений на информационные технологии, используемые в ИС налоговых органов и должна обеспечивать реализацию функций безопасности на всех этапах обработки информации, в том числе при техническом обслуживании и ремонте оборудования ИС налоговых органов.

6.3.3. Архитектура механизма поддержки СОБИ ФНС России

Механизм поддержки СОБИ ФНС России реализуется различными структурными подразделениями налоговых органов, которые, как правило, не участвуют непосредственно в процессе обработки информации или обслуживании ИС налоговых органов и не имеют единого подчинения на оперативном уровне. При этом всегда существуют широкие горизонтальные связи взаимодействия. Комплекс мер, реализуемых механизмом поддержки, направлен на усиление мер, реализуемых исполнительным механизмом, поэтому механизм поддержки СОБИ строится по матричной структуре, аналогичной структуре исполнительного механизма СОБИ (Рис. 13).

Меры, реализуемые механизмом поддержки СОБИ, структурируются по трем функциональным компонентам: организационная, инженерно-техническая и техническая.

Комплекс организационных мер составляют меры, определяемые организационно-распорядительными документами ФНС России и направленные на поддержание установленного порядка обеспечения безопасности информации. Учитывая, что данные мероприятия напрямую не связаны с процессом обработки информации и, как правило, затрагивают наиболее общие для всех подразделений налоговых органов вопросы, состав определяющих их организационно-распорядительных документов не входит в Политику ИБ ФНС России. Для формирования необходимых организационных мер требуется внесения изменений в действующие организационно-распорядительные документы ФНС России.

Комплекс инженерно-технических мер составляют меры, направленные на поддержание необходимых условий работы ИС налоговых органов и обеспечение общей защиты объектов. Такие меры определяются нормативными документами, техническими условиями, конструкторской документацией на сооружения и системы жизнеобеспечения объекта информатизации налоговых органов.

Комплекс технических мер составляют меры, направленные на создание и поддержание в постоянной готовности резервных мощностей, позволяющих обеспечить при необходимости быстрое устранение нештатных ситуаций при эксплуатации ИС налоговых органов.

Основные организационные, инженерно-технические и технические меры реализуемые механизмом поддержки приведены в Приложении № 8 к настоящей Концепции.

VII. Требования обеспечения безопасности информации в ФНС России

Точкой приложения усилий по защите информации является ИС. Для создания условий (оболочки), исключающих возможность противоправных действий с объектом защиты, предъявляются требования к защищенности (уровню защиты) ИС налоговых органов и окружению, в котором функционируют объекты защиты.

Требования данного раздела должны учитываться при подготовке технических заданий на проектирование и при проектировании ИС налоговых органов.

7.1. Выбор уровня защищенности информационных систем ФНС России

7.1.1. Общие положения по выбору класса защищенности

Выбор класса защищенности элементов ИС проводится с целью реализации принципа дифференцированного подхода к обеспечению безопасности информации. Класс защищенности определяет состав исполнительного механизма СОБИ и механизма его поддержки, обеспечивающих требуемый уровень безопасности объектов защиты ФНС России.

Допускаются разные классы защищенности для разных элементов (обособленных сегментов, подсистем, объектов) ИС налоговых органов. При выборе класса защищенности необходимо ориентироваться на стандартизированные классы защищенности автоматизированных систем,

определенные руководящими документами ФСТЭК России, что облегчает подбор СЗИ, имеющихся на рынке безопасности и позволяет упростить предъявление требований к организациям, участвующим в процессе межведомственного информационного обмена.

Классификация ИС (АС, отдельных АРМ), телекоммуникационных линий связи (при условии применения криптографической защиты информационного канала), обрабатывающих государственную тайну, осуществляется в соответствии с требованиями государственных регуляторов (ФСТЭК России и ФСБ России).

Классификация ИС налоговых органов, используемых для обработки персональных данных, осуществляется в соответствии с требованиями, устанавливаемыми уполномоченными федеральными органами исполнительной власти.

Классификация ИС налоговых органов, отнесенных к КСИИ, осуществляется с учетом степени важности данной ИС.

Набор функциональных компонент защиты, реализуемых исполнительным механизмом СОБИ и необходимых для обеспечения требуемого класса защищенности элементов ИС налоговых органов, может быть изменен (дополнен, сокращен относительно набора определенного руководящими документами) по результатам проведенного анализа и оценки актуальных угроз. При этом каждый факт изменения должен иметь документальное обоснование.

7.1.2. Базовый уровень защищенности ИС налоговых органов

Базовый уровень задает нижний предел требований для элементов ИС налоговых органов и определяет минимальный объем требований, обеспечивающий приемлемый уровень риска утраты конфиденциальности, целостности или доступности информации.

Сегменты ИС налоговых органов, предназначенные для обработки защищаемых ИР, не могут иметь уровень защищенности ниже базового.

В качестве базового уровня для ИС налоговых органов (обособленных сегментов), предназначенных для обработки ИР, составляющих государственную тайну, устанавливается класс защищённости 1Б, который выбирается исходя из следующих критериев:

в ИС налоговых органов одновременно обрабатывается и хранится информация разной степени секретности («совершенно секретно», «секретно»);

пользователи ИС налоговых органов имеют разные полномочия по доступу к информации, составляющей государственную тайну;

ИС налоговых органов являются многопользовательскими системами.

Базовый уровень для ИС налоговых органов, предназначенных для обработки информации, составляющей государственную тайну, подлежит обязательному уточнению на каждом объекте информатизации налоговых органов, с учетом степени секретности обрабатываемой информации и условий их расположения относительно постоянных представительств иностранных государств, обладающих правом экстерриториальности.

В качестве базового уровня для ИС налоговых органов (обособленных сегментов), предназначенных для обработки Конфиденциальных ИР и Открытых ИР устанавливается класс защищенности 1Г, который выбирается исходя из следующих критериев:

в ИС налоговых органов одновременно обрабатывается и хранится информация различных категорий конфиденциальности (налоговая, служебная, коммерческая тайна, персональные данные и др.)

пользователи ИС налоговых органов имеют разные полномочия по доступу к Конфиденциальным и Открытым ИР;

ИС налоговых органов являются многопользовательскими системами.

Для сегментов ИС налоговых органов, объединяющих хранилища (базы данных) персональных данных, в соответствии с установленным порядком проведения классификации информационных систем персональных данных (ИСПДн), устанавливается базовый уровень защищённости класса К2. Указанный уровень устанавливается с учетом следующих критериев:

в сегментах ИС налоговых органов, объединяющих хранилища персональных данных находятся персональные данные, позволяющие идентифицировать субъекта и получить о нем дополнительную информацию;

в сегментах ИС налоговых органов, объединяющих хранилища персональных данных находятся персональные данные более чем 10 000 субъектов персональных данных или персональные данные субъектов в пределах субъекта Российская Федерация или Российской Федерации в целом;

нарушение конфиденциальности и целостности персональных данных, хранимых в сегментах ИС налоговых органов, объединяющих хранилища персональных данных, может привести к негативным последствиям и ущербу для субъектов;

в сегментах ИС налоговых органов, объединяющих хранилища персональных данных, хранятся не обезличенные персональные данные субъектов.

Базовый уровень защищенности для сегментов ИС налоговых органов, объединяющих хранилища (базы данных) персональных данных может быть понижен до класса К3, в случае использования обезличенных персональных данных.

Для сегментов ИС налоговых органов, объединяющих рабочие станции пользователей, средства ввода и вывода информации, осуществляющих обработку персональных данных, базовый уровень защищенности устанавливается класса К3 и уточняется установленным порядком, с учетом способов обработки персональных данных, их объема и состава.

Применяемые в составе ИС налоговых органов средства обработки информации должны быть не ниже пятого класса защиты.

Программно-аппаратные средства межсетевого экранирования, применяемые для разграничения сегментов внутри ИС налоговых органов, должны быть не ниже четвертого класса защиты, а предназначенные для подключения к информационно-телекоммуникационным сетям международного информационного обмена (включая сеть Интернет) должны также удовлетворять требованиям ФСБ России.

Основные требования базового уровня, предъявляемые к ИС налоговых органов, приводятся в руководящих документах ФСТЭК России.

Элементы ИС налоговых органов, предназначенные для обработки объектов защиты, не могут иметь уровень защищенности ниже базового. В случае невозможности выделения элементов ИС налоговых органов, предназначенных для обработки информации различных уровней защищенности, в обособленные сегменты, класс защищенности таких сегментов (элементов) должен соответствовать высшему классу защищённости обрабатываемой информации.

В случае отнесения того или иного сегмента к КСИИ, для установления класса защищенности требуется определить степень важности информации для государства. Важность информации определяется по уровню негативных последствий в обществе в случае уничтожения (нарушитель ИБ или природные катаклизмы) консолидированных данных о финансовых поступлениях, например: может быть нарушена своевременность наполнения бюджетов и т.п.

Четвертый уровень важности КСИИ требований по защите информации не имеет.

Второй и третий уровни важности КСИИ предъявляют практически аналогичные требования к классу защищенности, как и требования к классу защищенности в системе обработки персональных данных. При этом дополнительно рассматриваются каналы утечки информации по ПЭМИН и физической защиты объекта.

Безопасность информации в КСИИ требует повышенных требований по катастрофоустойчивости и надежностным характеристикам.

Пересмотр класса защищенности элементов ИС налоговых органов производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых они были установлены.

7.2. Основные требования к СОБИ ФНС России

7.2.1. Требования к составу мероприятий, реализуемых СОБИ ФНС России

Исполнительный механизм в совокупности с механизмом поддержки СОБИ на физическом подуровне должны обеспечивать создание защищенной физической оболочки для объектов информатизации налоговых органов.

Исполнительный механизм СОБИ в совокупности с механизмом поддержки СОБИ на технологическом подуровне исполнительского уровня СОБИ должны обеспечивать создание защищенной программной и аппаратной оболочки для ИС ФНС России (защищенной платформы ИС налоговых органов). На этом подуровне обеспечивается:

защита ИР ФНС России, содержащих системное и прикладное программное обеспечение, необходимое для работы ИС налоговых органов;

защита Инфраструктурных ИР ФНС России, содержащих сведения по администрированию ИС налоговых органов.

Исполнительный механизм в совокупности с механизмом поддержки СОБИ на пользовательском подуровне должны обеспечить допуск к работе в ИС налоговых органов только авторизованных пользователей (принцип «свой - чужой») и создание защитной оболочки вокруг элементов ИС налоговых органов (рабочие станции, серверы) и индивидуальной среды деятельности каждого пользователя. На этом подуровне обеспечивается:

защита Инфраструктурных и Технологических ИР ФНС России, содержащих имена, пароли и другую идентификационную информацию пользователей ИС налоговых органов;

защита ИР, составляющих государственную тайну, Конфиденциальных и Открытых ИР ФНС России, содержащих защищаемую информацию;

защита информационных процессов программного обеспечения.

Исполнительный механизм СОБИ в совокупности с механизмом поддержки СОБИ на сетевом (локальном) подуровне исполнительского уровня СОБИ должны обеспечивать разделение ИР ФНС России и средств их обработки на сегменты, создание надежной защищенной оболочки по периметру сегментов, организацию защищенного обмена информацией между сегментами, а также

ограничение числа точек взаимодействия (точек входа/выхода) сегментов между собой. На этом подуровне обеспечивается:

защита Инфраструктурных ИР, содержащих адресную информацию ИС налоговых органов (скрытие топологии ИС налоговых органов);

защита Инфраструктурных ИР ФНС России, содержащих имена узлов телекоммуникационной инфраструктуры, пользователей, пароли доступа и другую идентификационную информацию);

защита информации, обрабатываемой в выделенных сегментах ИС налоговых органов и скрытие их топологии;

защита ИР, составляющих государственную тайну, Конфиденциальных и Открытых ИР ФНС России, содержащих защищаемую информацию;

защита информационных процессов программного обеспечения.

Исполнительный механизм в совокупности с механизмом поддержки СОБИ на канальном подуровне должны обеспечивать создание надежной защитной оболочки по внешнему периметру ИС налоговых органов и организацию защищенного межведомственного обмена информацией с другими органам государственной власти, а также защищенного обмена информацией с удаленными и мобильными пользователями ИС налоговых органов и, при необходимости, с внешними пользователями. На этом подуровне обеспечивается:

защита и скрытие трафика в каждом из каналов его распространения;

защита ИР, составляющих государственную тайну, Конфиденциальных и Открытых ИР ФНС России, содержащих защищаемую информацию;

защита информации, передаваемой по каналам связи.

Конкретный состав мероприятий, подлежащих реализации на различных подуровнях исполнительского уровня СОБИ приведен в Приложении № 9 к настоящей Концепции.

7.2.2. Основные требования к СиЗИ

СиЗИ формируется на программно-аппаратной (программной) платформе, способной обеспечить функционирование всех ее подсистем. СЗИ, используемые в СиЗИ, должны быть совместимы между собой и с имеющимися программно-аппаратными средствами ИС налоговых органов.

СиЗИ должна обеспечивать круглосуточную эксплуатацию технических средств, предназначенных для реализации поставленных целей ИБ. Стойкость и надежность СиЗИ не должна зависеть от стойкости и надежности отдельно взятого СЗИ.

СиЗИ должна строиться на основе использования:

на физическом подуровне - технических средств охраны, видеонаблюдения, разграничения доступа

на технологическом подуровне - встроенных функций защиты общесистемного программного обеспечения (ОС, СУБД), в совокупности со специальными техническими средствами защиты;

на пользовательском подуровне - программных и/или программно-аппаратных средств защиты от НСД к информации в совокупности со встроенными функциями защиты общесистемного программного обеспечения (ОС, СУБД) а также средств управления потоками информации между пользователями;

на сетевом (локальном) подуровне - программно-аппаратных средств повышенной аутентификации и защиты от НСД к информации и использования между сегментами программных или программно-аппаратных средств, использующих технологии межсетевого экранирования, обеспечивающих разграничение доступа к ИР ФНС России;

на канальном уровне - программно-аппаратных средств, использующих технологии межсетевых экранов, и средств создания защищенного от несанкционированных действий виртуального канала связи (VPN-технологий) и не снижающих установленный уровень защищенности ИС налоговых органов.

Конкретный состав СЗИ и места их возможного размещения, а также основные требования к ним, позволяющие решить задачи ИБ относительно каждого подуровня исполнительского уровня СОБИ, приведены в Приложении № 10 к настоящей Концепции.

Конкретный набор функций безопасности, которые должны быть реализованы СЗИ, входящими в СиЗИ, определяется организационно-распорядительным документом второго (оперативного) уровня Политики ИБ: «Общие технические требования по обеспечению безопасности информации при разработке и внедрении прикладных систем ФНС России» (Стандарт ФНС России).

7.2.3. Дополнительные требования по локализации ИР ФНС России

Для локализации ИР ФНС России, требующих защиты, проводится сегментирование ИС налоговых органов.

При сегментировании ИС налоговых органов могут выделяться открытые, закрытые, буферные, удаленные (открытые и закрытые) сегменты. Состав элементов ИС налоговых органов, входящих в конкретные типы сегментов, и образуемые ими контуры взаимодействия приведены в Приложении № 11 к настоящей Концепции.

Сопряжение сегментов между собой осуществляется только через специальные средства защиты, размещаемые в точках их сопряжения и не снижающие наивысший установленный для сегмента ИС налогового органа класс защищенности. Количество точек сопряжения одного сегмента с другими должно быть минимально необходимым (ограниченным).

Закрытые сегменты ИС налоговых органов (сегменты более высокого класса защищенности) располагаются внутри открытых сегментов (сегментов более низкого класса защищенности). При этом, для пользователей открытого сегмента, весь закрытый сегмент должен быть воспринимаем как один пользователь (скрытие топологии закрытого сегмента). Закрытые сегменты могут сопрягаться только с открытыми сегментами и не могут быть непосредственно сопряжены с удаленными сегментами или с глобальными информационно-телекоммуникационными сетями общего пользования (включая сеть Интернет).

Удаленный сегмент сопрягается только с открытыми или буферными сегментами. Допускается сопряжение закрытого удаленного сегмента непосредственно с закрытым сегментом ИС налогового

органа при наличии специально выделенного канала связи и применения средств канального шифрования информации.

Создаваемая СОБИ ФНС России должна обеспечивать формирование матрицы доступа, определяющей (и ограничивающей) конкретные полномочия пользователей различных сегментов ИС налоговых органов по обращению к конкретным ИР ФНС России и предусматривающей следующие правила:

пользователи открытого сегмента не должны иметь доступа к ИР и процессам закрытого сегмента. Пользователи открытого сегмента могут иметь доступ к ИР глобальных информационно-телекоммуникационных сетей общего пользования (включая сеть Интернет);

пользователи закрытого сегмента могут иметь доступ к ИР и процессам открытого сегмента;

пользователи закрытого сегмента не должны иметь прямого доступа к информационным ресурсам глобальных информационно-телекоммуникационных сетей общего пользования;

пользователи открытого и закрытого удаленного сегмента при осуществлении обмена информацией должны иметь доступ только к открытому или буферному сегментам ИС. При этом доступ к ИР глобальных информационно-телекоммуникационных сетей общего пользования запрещается;

пользователи открытого удаленного сегмента, при осуществлении обмена информацией, могут иметь прямой доступ к глобальным ИС через автономные средства передачи информации (модем). При этом доступ пользователей удаленного сегмента к закрытому и открытому сегментам запрещается, а доступ к буферному сегменту осуществляется на правах внешнего пользователя, не входящего в состав ИС;

пользователям закрытого удаленного сегмента запрещается иметь прямой доступ к ИР глобальных информационно-телекоммуникационных сетей общего пользования.

7.2.4. Дополнительные требования при использовании технологий виртуализации

Виртуальные технологии могут применяться только в пределах ИС налоговых органов и телекоммуникационной инфраструктуры, находящихся в ведении ФНС России. Местоположения

физических серверов, доступных для запуска виртуальной машины должно быть ограничено Центрами обработки данных (ЦОД) ФНС России.

При использовании в ИС налоговых органов технологий виртуализации должна быть обеспечена сегрегация используемых, передаваемых или хранимых в виртуальной среде данных между разными виртуальными машинами, исключающая, в том числе и для администраторов ИС (администраторов виртуальной среды) налоговых органов, возможность получения внешнего доступа к оперативной памяти работающих виртуальных машин и областям виртуальной среды, предназначенным для хранения защищаемой информации.

Используемое для создания виртуальной среды программное обеспечение гипервизора (виртуализатора) должно пройти оценку соответствия (сертификацию) на отсутствие недекларированных возможностей.

Для обеспечения требуемого уровня сегрегации данных и защиты информации при использовании технологий виртуализации, в рамках существующей СиЗИ ИС налоговых органов должно быть обеспечено:

в рамках контура ПДС исполнительного механизма СОБИ - доверенный контроль целостности виртуальной среды;

в рамках контура ИАС исполнительного механизма СОБИ - аутентификация и авторизация рабочих станций (АРМ) пользователей;

в рамках контура КДС исполнительного механизма СОБИ - контролируемое пользователем прозрачное шифрование виртуальных дисков критичных серверов;

в рамках контура ЗПИ исполнительного механизма СОБИ - контролируемая пользователем защита виртуальных сетевых взаимодействий.

При обеспечении доверенного контроля целостности виртуальной среды должна осуществляться доверенная загрузка виртуальной среды. При этом должно контролироваться соответствие контрольных сумм текущего образа программного обеспечения гипервизора (виртуализатора)

сертифицированному эталону. Ключи аутентификации, контрольные суммы программного обеспечения должны храниться в защищенном виде на независимом аппаратно-программном элементе, обеспечивающем защищенный канал доступа к результатам контроля.

При аутентификации и авторизации рабочих станций (АРМ) пользователей должен быть обеспечен контроль целостности программного обеспечения рабочих станций пользователей ИС налоговых органов, с которых осуществляется доступ в виртуальную среду, аутентификация пользователей и создан защищенный виртуальный канал для передачи информации между виртуальной средой и рабочей станцией пользователя ИС налоговых органов.

При обеспечении контролируемого пользователем прозрачного шифрования виртуальных дисков критичных серверов, защищаемая информация, а также ее резервные копии, должны храниться в зашифрованном виде на диске пользовательской виртуальной машины, как в выключенном, так и в работающем состоянии. При этом, доступом к ключу шифрования должен управлять владелец виртуальной машины. Решение о предоставлении доступа к ключу шифрования владелец виртуальной машины должен принимать на основании аутентификации аппаратно-программной платформы физического сервера и результатов контроля целостности виртуализатора. Загрузка ключей шифрования должна осуществляться с рабочей станции пользователя ИС налогового органа с применением съемного носителя (токена, смарт-карты).

Для обеспечения контролируемой пользователем защиты виртуальных сетевых взаимодействий, позволяющих сегрегировать передаваемую внутри виртуальной среды информацию и обеспечить защиту сетевых взаимодействий от влияния администраторов виртуальной среды, для всех серверов на которых размещаются защищаемые ИР ФНС России, в виртуальной среде должна быть обеспечена возможность создания выделенной защищенной виртуальной подсети по схеме «точка-точка».

7.2.5. Дополнительные требования использования криптографических средств

Средства криптографической защиты информации (СКЗИ) могут применяться для обеспечения конфиденциальности защищаемой информации, подтверждения подлинности передаваемых сообщений (придания юридической значимости электронным документам) или контроля целостности ИР.

Необходимость применения СКЗИ при защите ИР ФНС России определяется руководством ФНС России, как обладателем ИР.

Применяемые для защиты информации в ФНС России СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом законодательством Российской Федерации. Применяемые СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правил работы с ней, а также обоснование необходимого организационно-штатного обеспечения. А также иметь строгий регламент использования ключей, предполагающий контроль со стороны администратора ИБ за действиями пользователей ИС налоговых органов на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя).

Применяемые в ФНС России СКЗИ должны обеспечивать:

встраивание в действующую в налоговых органах технологическую схему обработки электронных сообщений;

взаимодействие с прикладным программным обеспечением ИС налоговых органов на уровне обработки запросов на криптографические преобразования и выдачи результатов;

реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей или при переходе ИС налоговых органов в нештатный режим работы.

При применении СКЗИ в ИС налоговых органов должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечение целостности программного обеспечения для всех элементов ИС, имеющих в своем составе СКЗИ.

Все криптографические ключи должны быть защищены от несанкционированной модификации, кражи, разрушения и раскрытия. Используемое для генерации, сохранения и архивирования ключей оборудование (средства) должно быть физически защищено. Для уменьшения вероятности компрометации ключевого материала, необходимо, чтобы ключи имели определённые даты активации и деактивации, чтобы их могли использовать только ограниченный период времени.

Порядок генерации, распределения, хранения, уничтожения, учета криптографических ключей, а также порядок проведения периодических проверок выполнения пользователями требований по

хранению и эксплуатации криптографических ключей определяется в соответствии с методическими рекомендациями ФСБ России.

Для хранения отчуждаемых носителей ключевой информации должны использоваться индивидуальные хранилища (сейфы, шкафы и т.п.). Ключи должны храниться в специальной упаковке, исключающей возможность несанкционированного доступа к ним.

Криптографические ключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптографические ключи, подлежат немедленному выводу из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

7.2.6. Дополнительные требования при обработке ИР, содержащих государственную тайну

При обработке ИР, содержащих государственную тайну, должны выполняться рекомендации регуляторов по их размещению, электропитанию и использованию.

Для обработки ИР, составляющих государственную тайну, должны применяться средства обработки информации, сертифицированные по требованиям безопасности информации, либо прошедшие специальные исследования и имеющие предписания на эксплуатацию, требования которых реализованы на объекте информатизации налоговых органов.

Для объектов информатизации налоговых органов, необходимые меры защиты ИР, составляющих государственную тайну, должны быть определены по результатам обследования объекта и результатам специальных исследований средств обработки информации и должны быть указаны в предписаниях на их эксплуатацию. При невозможности выполнения требований предписания, средства обработки информации должны быть доработаны по требованиям безопасности информации, либо заменены на другие, имеющие параметры, которые позволяют реализовать требования безопасности на объектах налоговых органов.

Сети и средства передачи секретной информации, включая аппаратуру обработки и передачи информации и линии передачи данных, должны располагаться в пределах контролируемой зоны объекта информатизации. Передача секретной информации по линиям, расположенным за пределами контролируемой зоны, разрешается только в случае использования защищенных линий связи, аттестованных в установленном порядке, а также сертифицированных СКЗИ.

Запрещается обработка секретной информации в ИС, имеющих непосредственный выход в международные открытые телекоммуникационные сети (включая сеть Интернет). Допускается подключение сегментов ИС налоговых органов, обрабатывающих ИР, составляющие государственную тайну, к другим сегментам ИС налоговых органов, в том числе и применяемым для обработки открытой информации, расположенным в пределах контролируемой зоны объектов информатизации налоговых органов, при следующих условиях:

между сегментами должны быть реализованы средства разграничения доступа, исключающие возможность получения доступа пользователей открытых сегментов к секретным данным;

в режиме передачи секретной информации сегменты ИС, не предназначенные для обработки ИР, составляющих государственную тайну, должны отключаться, либо блокироваться от прохождения в нее информативных сигналов, несущих секретную информацию.

При несоблюдении этих условий объединенные сегменты ИС налоговых органов должны рассматриваться как единая ИС, требования по защите информации в которой от утечки по каналам ПЭМИН должны определяться в соответствии с высшей степенью секретности информации.

Помещения, в которых размещаются средства обработки ИР, составляющих государственную тайну, должны располагаться в пределах контролируемой зоны объектов информатизации налоговых органов и должны быть оборудованы техническими средствами охраны, обеспечивающими уровень защиты, соответствующий степени секретности. В этом случае применение СКЗИ не является обязательным. При отсутствии возможности оборудования помещений техническими средствами охраны соответствующего уровня защиты, в сегментах ИС налоговых органов, обрабатывающих секретную информацию, должны использоваться сертифицированные СКЗИ.

Учет, хранение и выдача пользователям ИС налоговых органов секретных носителей информации, учтенной бумаги для распечаток (в случае отсутствия программной реализации печати учетных реквизитов и контроля за выдачей распечаток), паролей и ключей для СЗИ, осуществляется в соответствии с требованиями секретного делопроизводства. Учет, хранение, уничтожение пришедших в негодность магнитных носителей информации производится в соответствии с порядком, установленным для секретных изделий.

7.2.7. Дополнительные требования к катастрофоустойчивости объектов ФНС России

Обеспечение катастрофоустойчивости телекоммуникационной инфраструктуры ФНС России не является задачей обеспечения ИБ ФНС России и относится к сфере обеспечения безопасности критически важных объектов. Вместе с тем, катастрофоустойчивость телекоммуникационной инфраструктуры и ЦОД ФНС России может существенно снизить угрозы ИБ при обработке и передаче информации между объектами налоговых органов. Мероприятия по обеспечению катастрофоустойчивости, как правило, реализуются подразделениями налоговых органов, непосредственно не участвующих в обработке информации (службы эксплуатации объектов налоговых органов), на этапе капитального строительства объектов информатизации налоговых органов.

Создаваемые объекты информатизации налоговых органов (ЦОД ФНС России и объекты телекоммуникационной инфраструктуры ФНС России) должны проектироваться по уровню соответствующему уровню 3 стандарта TIA-ETA-942 для всех составных частей инфраструктуры, с учетом поддержания требуемого уровня на протяжении срока эксплуатации не менее 10 лет и с учётом возрастания нагрузки с течением времени. При этом должны обеспечиваться:

плановая деятельность объектов информатизации налоговых органов без нарушения нормальной работы технических средств обработки информации, размещаемых на этих объектах;

возможность обеспечения требуемой вводной мощности электроэнергии для объектов информатизации налоговых органов;

наличие нескольких путей (каналов) для распределения электропитания и охлаждения, один из которых должен находиться в активном состоянии;

достаточные мощности и распределительные возможности, позволяющие при загруженности одного пути (канала) одновременно осуществлять обслуживание или тестирование другого пути (канала);

допустимое время простоя объекта информатизации налогового органа в год не более 1,6 часа;

возможность набора квалифицированного персонала для службы эксплуатации объектов налоговых органов;

возможность размещения в непосредственной близости от объектов информатизации налоговых органов резервных электрогенераторов и топливохранилищ;

доступность телекоммуникационной инфраструктуры, близость объектов информатизации налоговых органов к местам пиринга трафика операторов телематических услуг;

удалённость объектов информатизации налоговых органов от мест возможных затоплений и других стихийных бедствий;

близость к основным транспортным магистралям (не менее 100 м) и крупным городским районам.

Для поддержания требуемого уровня катастрофоустойчивости для важнейших объектов налоговых органов необходимо:

провести инвентаризацию объектов налоговых органов и телекоммуникационной инфраструктуры ФНС России, выявить наиболее критичные с точки зрения катасрофоустойчивости объекты и определить уровень их катастрофоустойчивости;

разработать стратегию управления рисками, проводить идентификацию и анализ неблагоприятных воздействий на объекты налоговых органов и телекоммуникационную инфраструктуру ФНС России;

разработать План обеспечения катастрофоустойчивости объектов налоговых органов и телекоммуникационной инфраструктуры ФНС России;

обеспечить внедрение необходимых для поддержания катастрофоустойчивости объектов налоговых органов изменений в техническом, организационном и информационном обеспечении ФНС России, предусмотренных Планом обеспечения катастрофоустойчивости.

VIII. Особенности обеспечения безопасности информации в некоторых ситуациях

8.1. Обеспечение безопасности информации при использовании международных информационно-телекоммуникационных сетей общего пользования, включая сеть Интернет

Особенности обеспечения безопасности ИР ФНС России при сопряжении ИС ФНС России с международными информационно-телекоммуникационными сетями (сетями связи общего пользования), включая сеть Интернет (далее - ССОП) обусловлены тем, что пользователи ИС налоговых органов могут использовать ССОП в качестве:

транспортной среды при межведомственном обмене информацией между собой и с другими органами государственной власти (транспортная задача);

средства предоставления открытых общедоступных ИР ФНС России, любому внешнему пользователю, не принадлежащему к ИС налоговых органов (портальная задача);

средства получения пользователями ИС ФНС России информации, содержащейся в ИР ССОП (информационная задача).

8.1.1. Сопряжение ИС налоговых органов с ССОП

Согласно существующим требованиям, при необходимости подключения ИС налоговых органов к ССОП необходимо использовать специально предназначенные для этого средства защиты информации, в том числе СКЗИ, прошедшие в установленном законодательством Российской Федерации порядке сертификацию. Выполнение данного требования является обязательным.

ССОП могут сопрягаться только с буферным сегментом ИС налоговых органов, в пределах которого, в точках его сопряжения с коммутационным оборудованием провайдеров телематических услуг, должен быть установлен сервер, реализующий функции Proxy-сервера и NAT-технологию и обеспечивающий скрытие адресного пространства (топологии) ИС налоговых органов.

Встроенные в программное обеспечение коммуникационных серверов, коммутаторов и маршрутизаторов, межсетевых экранов, СЗИ и средства разграничения доступа к информации, установленные в точках сопряжения с ССОП, должны быть корректно настроены и исключать возможность чтения, изменения и/или разрушения управляющей информации, хранящейся в этом оборудовании (таблиц маршрутизации, полномочий пользователей, запрещения доступа по определённым портам, ограничения доступа по времени и пр.), накапливать статистику использования сетевых ресурсов и попыток НСД в периметр ИС налоговых органов.

СЗИ, используемые на серверах буферного сегмента ИС налоговых органов, должны обеспечивать контроль целостности имеющегося на них программного обеспечения и ИР ФНС России, их периодический мониторинг для устранения возможности их компрометации при реализации портальной задачи.

8.1.2 Особенности разрешения информационной задачи

При необходимости организации доступа пользователям закрытого сегмента ИС налоговых органов к ИР ССОП (информационная задача), в пределах открытого сегмента ИС налоговых органов должен быть размещен специальный сервер (обособленный сегмент открытого сервера), на котором специально уполномоченным лицом (администратором ИБ) по запросам пользователей закрытого сегмента эмулируются необходимые ИР ССОП. Количество таких ИР должно быть ограничено служебной необходимостью, а сами ИР до их эмуляции, должны быть проверены и освобождены от вредоносных программ, программ не установленного назначения и программ, не несущих информативную нагрузку (реклама, баннеры, апплеты).

Доступ пользователей открытого сегмента ИС налоговых органов к ИР ССОП должен осуществляться через специальный сервер (обособленный сегмент открытого сервера), размещённый в пределах открытого сегмента, реализующий функции Proxy-сервера и NAT-технологию и обеспечивающий сокрытие адресного пространства (топологии) ИС налоговых органов.

8.1.3. Особенности разрешения портальной задачи

Внешние пользователи ИС налоговых органов, обращающиеся через ССОП (портальная задача) к общедоступным ИР ФНС России, должны пройти процедуру предварительной регистрации, проверки их адреса и получения персонального пароля. Доступ таких пользователей в пределы буферного сегмента ИС налоговых органов должен осуществляться только по полученному паролю и после процедуры идентификации и аутентификации.

Внешние пользователи не должны иметь доступа к ИР ФНС России, процессам и пользователям открытого и закрытого сегментов ИС налоговых органов, а также права записи и модификации (изменения) открытых ИР ФНС России, хранящихся на серверах буферного сегмента.

8.1.4 Особенности разрешения транспортной задачи

При использовании пользователями ИС налоговых органов в ходе межведомственного информационного обмена, необходимого для исполнения государственных функций и оказания

государственных услуг, ССОП в качестве транспортной среды (транспортная задача) необходимо создавать защищенные виртуальные каналы обмена информацией и применять СКЗИ.

Обмен информацией, между пользователями ИС налоговых органов и пользователями удаленного сегмента осуществляется с применением СКЗИ, обеспечивающих имитостойкость, соответствующую степени конфиденциальности передаваемой информации. При этом должны быть выполнены организационные меры обеспечения безопасности СКЗИ, предъявляемые ФСБ России.

При обеспечении транспортной задачи, пользователи открытого и закрытого удаленного сегментов ИС налоговых органов могут иметь доступ только к открытому или буферному сегментам. При этом, доступ к ИР ССОП (реализация информационной задачи) этих пользователей запрещается.

8.2. Обеспечение безопасности информации при привлечении налоговыми органами внешних (аутсорсинговых) организаций

Для снижения издержек на обслуживание ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России могут привлекаться внешние специализированные организации - поставщики услуг (аутсорсинговое обслуживание). Вместе с тем, такой подход создаёт дополнительные риски нарушения конфиденциальности, целостности или доступности защищаемой информации.

Привлечение поставщиков услуг для обеспечения ИБ возможно только на операционном и исполнительском уровнях СОБИ.

8.2.1. Требования, учитываемые при заключении контракта с поставщиком услуг

В случае аутсорсинга регламентация вопросов ИБ носит обязательный характер, поскольку зоны полномочий и ответственности должны быть определены заранее, и в случае инцидента нужно четко идентифицировать ответственных и определить виновных.

Требования безопасности, в случае когда ФНС России передает для управления и контроля все или некоторые из элементов ИС налоговых органов, должны быть указаны в контракте, согласованном между сторонами и учитывающем:

наличие соглашения о неразглашении поставщиком услуг информации ограниченного доступа/распространения, ставшей известной ему в ходе исполнения договорных обязательств;

выполнение требований по защите информации, установленные законодательством Российской Федерации;

достижение договоренностей, обеспечивающих уверенность в том, что все стороны, включая субподрядчиков, осведомлены о своих обязанностях, касающихся безопасности;

возможность обеспечения и тестирования параметров целостности и конфиденциальности ИР ФНС России;

типы физических и логических методов по управлению ИБ, используемых при предоставлении необходимого доступа к конфиденциальной информации ФНС России сторонним пользователям аутсорсинговой организации;

обеспечение доступности сервисов в случае бедствия (наступления форс-мажорных обстоятельств);

уровни физической безопасности, которые должны быть обеспечены в отношении оборудования, используемого в рамках аутсорсинга;

соблюдение поставщиком услуг требования законодательства Российской Федерации о лицензировании, сертификации, требования трудового и налогового законодательства;

право на проведение аудита деятельности поставщика услуг со стороны ФНС России;

возможность расторжения договора с аутсорсинговой организацией в одностороннем порядке;

необходимость разработки регламента доступа ФНС России к арендуемым мощностям и каналам связи;

необходимость разработки регламента информирования ФНС России о попытках НСД при использовании арендуемого оборудования и каналов связи;

необходимость выполнения технических требований по защите информации, действующих в ФНС России.

8.2.2. Требования к поставщику услуг (аутсорсинговой организации)

Поставщик услуг (аутсорсиноговая организация) должен удовлетворять требованиям, установленными Федеральным законом от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд», Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании» и нормативными правовыми актами Российской Федерации.

8.3. Обеспечение безопасности информации в ФНС России при неавтоматизированной обработке

Обработка информации ограниченного доступа (конфиденциальной), в том числе извлеченной из ИС налоговых органов, считается осуществленной без использования средств автоматизации (неавтоматизированной), если действия с информацией (использование, уточнение, распространение, уничтожение) осуществляются сотрудниками ФНС России без помощи средств вычислительной техники (СВТ). Обработка электронных копий бумажных конфиденциальных документов (сканы, цифровые фотоизображения) с применением СВТ относится к автоматизированной обработке.

При неавтоматизированной обработке информации ограниченного доступа в ФНС России необходимо обеспечить специальные условия хранения, обработки и обращения документов, содержащих информацию ограниченного доступа, гарантирующие надежную защиту как самих документов (материальных носителей), так и содержащейся в них конфиденциальной информации. Это обеспечивается:

введением персональной ответственности сотрудников ФНС России за учет, сохранность конфиденциальных документов и порядок обращения с ними;

разработкой в ФНС России регламентированной технологии:

издания и обработки конфиденциальных документов, в том числе на стадии подготовки черновиков и проектов документов, определением состава издаваемых документов и содержащейся в них конфиденциальной информации, включающей (но не ограничиваясь):

- определением порядка работы с документами ограниченного доступа в специально выделенных помещениях налоговых органов;

- определением порядка передачи документов ограниченного доступа в случае ухода сотрудника ФНС России в отпуск, командировку, при увольнении и т.д.;

- определением порядка пересылки документов ограниченного доступа, создание реестровой системы передачи конфиденциальных документов;

- созданием архивов документов ограниченного доступа, проведением регулярной экспертизы ценности документов и оценки возможности снятия отметки грифа конфиденциальности;

- определением порядка уничтожения документов ограниченного доступа;

введением в ФНС России требований к условиям хранения документов ограниченного доступа и обращения с ними:

- организацией обязательного поэкземплярного и полистного учета всех документов, содержащих сведения ограниченного доступа, а также проектов и черновиков таких документов;

- определением полного состава регистрационных данных о каждом документе, содержащем сведения ограниченного доступа (дата создания, получения, исполнения; регистрационный номер; фамилия, имя, отчество исполнителя, адресата; права доступа; степень конфиденциальности; количество листов и т.д.);

- организацией системы фиксации движения и местонахождения документов ограниченного доступа в налоговых органах;

- организацией хранения конфиденциальных документов на рабочих местах сотрудников ФНС России;

- организацией хранения документов ограниченного доступа в архивах налоговых органов;

созданием в ФНС Росси разрешительной системы доступа к документам ограниченного доступа и делам, обеспечивающей правомерное и санкционированное ознакомление с ними:

- разделение документов по степени конфиденциальности;

- присвоение каждому документу грифа конфиденциальности;

- разграничение права работы с документами ограниченного доступа;

- запрет несанкционированного выноса документов ограниченного доступа;

- принятие организационных мер, исключающих необоснованное ознакомление с документами сотрудников ФНС России, не имеющих полномочий.

проведение руководителями подразделений налоговых органов систематических проверок наличия конфиденциальных документов у исполнителей.

Сотрудники ФНС России, осуществляющие неавтоматизированную обработку информации ограниченного доступа, должны быть проинформированы об особенностях и правилах осуществления такой обработки, установленных организационно-распорядительными документами ФНС России.

8.4. Обеспечение безопасности информации при переходе к ИС налоговых органов нового поколения

8.4.1 Факторы, влияющие на безопасность информации при модернизации систем

В период модернизации ИС налоговых органов необходимо учитывать следующее:

в существующих к моменту модернизации ИС налоговых органов и телекоммуникационной инфраструктуре ФНС России имеются средства защиты информации, позволяющие решать локальные задачи защиты ИР ФНС России;

в налоговых органах имеются организационно-распорядительные документы и проводятся мероприятия, направленные на обеспечение ИБ; сложились устоявшиеся связи взаимодействия между подразделениями налоговых органов при решении задач ИБ;

имеющиеся СЗИ и проводимые мероприятия по обеспечению ИБ составляют локальную систему обеспечения безопасности налоговых органов, однако требуемый уровень защищенности ИС налоговых органов не в полной мере обеспечивается;

в структуре ФНС России развернут Удостоверяющий центр ФНС России, обеспечивающий юридически значимый электронный документооборот между налоговыми органами и при взаимодействии с другими органами государственной власти;

размещение элементов ИС налоговых органов нового поколения осуществляется в основном на действующих объектах информатизации налоговых органов, имеющих устоявшуюся инфраструктуру обеспечения деятельности объектов;

модернизация ИС налоговых органов не затрагивает изменения состава объектов защиты и субъектов информационного обмена и, как следствие, не требует существенных изменений организационной базы и механизма поддержки СОБИ ФНС России;

основные изменения, при переходе к ИС налоговых органов нового поколения, касаются исполнительского механизма СОБИ ФНС России;

в ходе модернизации ИС налоговых органов будет произведена консолидация локальных ИР ФНС России в Центрах обработки данных (ЦОД);

при модернизации ИС налоговых органов ожидается резкое увеличение обмена конфиденциальной информацией по каналам связи телекоммуникационной инфраструктуры ФНС России.

8.4.2. Особенности обеспечения безопасности информации при модернизации систем

Положения Концепции в полном объеме применимы при организации защиты информации как для существующих ИС налоговых органов, так и для ИС нового поколения. При этом введение положений данной Концепции, отличных от существующих на момент принятия Концепции, осуществляется постепенно в ходе модернизации объектов налоговых органов.

При переходе к ИС нового поколения, мероприятия по обеспечению ИБ в налоговых органах должны являться составной частью работ по реконструкции и эксплуатации объектов информатизации налоговых органов.

На период перехода к ИС нового поколения, существующие ИС налоговых органов должны рассматриваться как локальные сегменты единой ИС ФНС России, общая архитектура СОБИ которой представляет собой совокупность самостоятельных СОБИ налоговых органов (территориальных сегментов), объединенных едиными правилами использования защищаемых ИР ФНС России.

Работы по обеспечению ИБ при модернизации объектов информатизации налоговых органов выполняются в соответствии с заданием на проектирование. Раздел задания на проектирование, содержащий требования по защите, оформляется отдельным документом и разрабатывается подразделением информационной безопасности центрального аппарата ФНС России при участии проектной организации, имеющей лицензию ФСТЭК России на соответствующий вид деятельности. Решения по обеспечению ИБ, разрабатываемые в проектах, не должны противоречить требованиям настоящей Концепции.

В период перехода к ИС нового поколения, каждая существующая самостоятельная СОБИ налогового органа, исходя из принципа детерминированности, должна иметь архитектуру СОБИ, основанную на наличии полного набора функциональных контуров СОБИ и решать поставленные задачи относительно автономно. При этом взаимодействие самостоятельных СОБИ налоговых органов различного уровня осуществляется на уровне контуров управления информационной безопасности (контуров УИБ) и установления единых регламентов защиты информации. Это предполагает так же

создание в каждом территориальном сегменте (налоговом органе) собственной системы комплексного администрирования.

На завершающем этапе перехода к ИС налоговых органов нового поколения, после формирования функциональных контуров СОБИ ФНС России на федеральном уровне, включением в их состав функциональных контуров самостоятельных СОБИ налоговых органов создается единая СОБИ ФНС России и централизованная система УИБ и мониторинга событий безопасности.

СОБИ, создаваемая при переходе к ИС нового поколения, должна унаследовать правила использования защищаемых ИР ФНС России, применяемые в действующих ИС налоговых органов.

При замене технических СЗИ на средства нового поколения, вывод из действия существующих средств защиты осуществляется только после установки, настройки и оценки соответствия требованиям безопасности новых средств защиты информации.

8.4.3. Особенности обеспечения безопасности информации на стадии проектирования

Технический проект СОБИ должен содержать технические решения для исполнительного механизма СОБИ и состав организационных мер для механизма поддержки СОБИ, которые должны быть реализованы на этапе модернизации. Разработку рабочего проекта СОБИ осуществляет проектная организация, имеющая лицензии ФСТЭК России и ФСБ России на соответствующие виды деятельности.

К разработке могут также привлекаться субподрядные проектные организации при условии наличия у них соответствующих лицензий. Субподрядные проектные организации участвуют в разработке технических решений по заданиям проектной организации, которые не должны раскрывать цель, замысел обеспечения ИБ проектируемого объекта информатизации налоговых органов.

Технические решения разрабатываются и оформляются в соответствии с требованиями действующих стандартов, норм и правил. В чертежах и пояснительных записках, при оформлении проектной документации не должно раскрываться истинное назначение технических решений. Все обоснования технических решений, принятых в разделах рабочего проекта, приводятся в отдельном томе общей пояснительной записки. В остальной проектной документации, при необходимости, дается только ссылка на данный том. Структура, порядок и глубина изложения отдельного тома определяется подразделением информационной безопасности центрального аппарата ФНС России. К

ознакомлению с данными материалами допускается ограниченный круг лиц с разрешения подразделения информационной безопасности центрального аппарата ФНС России.

Проектная документация по обеспечению ИБ, при необходимости, может проходить экспертизу во ФСТЭК России или ФСБ России.

IX. Мониторинг и контроль состояния безопасности информации

9.1. Мониторинг состояния обеспечения безопасности информации

Мониторинг обеспечения безопасности информации проводится с целью объективного подтверждения реального состояния защищенности ИС налоговых органов, а также с целью контроля работоспособности исполнительных механизмов СОБИ, мониторинга сетевой топологии ИС и установленных сервисов, анализа трафика информационного обмена для обнаружения и протоколирования сетевых событий, сбора критичной информации и обнаружения уязвимостей для предотвращения инцидентов, обнаружения вторжений и аномальной активности пользователей ИС налоговых органов, оценки защищенности телекоммуникационной инфраструктуры ФНС России.

Мониторинг осуществляется силами и средствами СУИБ ФНС России. Процедуры мониторинга необходимы для создания гарантированной безопасной среды, в которой пользователи ИС налоговых органов, выполняют только те действия, которые они уполномочены выполнять.

Мониторинг предполагает постоянное наблюдение за состоянием ИС налоговых органов, анализа полученных данных и прогнозирования возможных критичных изменений состояния безопасности информации, возникновения инцидентов и нарушений режима защиты ИР ФНС России.

Для анализа трафика информационного обмена, обнаружения сетевых событий, сбора критичной информации, обнаружения аномальной активности пользователей ИС налоговых органов, идентификации ошибок и нарушений, установленных режимов защиты информации, должны использоваться журналы мониторинга (журналы оператора, администратора, системный журнал и журнал регистрации ошибок, лог-файлы). Контроль (обзор) журналов мониторинга позволяет собирать статистику нарушений и/или отклонений в эксплуатации ИС налоговых органов от заданного режима функционирования, определять способы локализации проблем и недопущения нарушений в дальнейшем.

Журналы мониторинга должны создаваться и сохраняться в течение установленного периода времени. Журналы мониторинга, содержащие записи пользовательских действий, регистрирующие

исключения, ошибки и другие информационные событий, в том числе и сообщения от СиЗИ и СЗИ, должны использоваться в ходе проводимых расследований инцидентов, нарушений правил доступа и использования ИС налоговых органов. Данные журналов мониторинга могут содержать конфиденциальную информацию и другие защищаемые сведения, как о легальных процессах и пользователях ИС налоговых органов, так и о нарушителях. Средства регистрации событий и ведения журналов мониторинга должны быть защищены от вмешательства в их работу и возможностей получения к ним несанкционированного доступа.

Данные мониторинга, касающиеся контроля состояния критичных процессов ИС налоговых органов, должны архивироваться в соответствии с принятой в ФНС России процедурой. Сохраненные данные должны обеспечивать доказательную базу для разбора возникающих проблем и инцидентов, в том числе и связанных с нарушениями Политики ИБ.

Уровень мониторинга необходимого для контроля конкретных технических средств обработки информации определяется по результатам оценки уровня информационных рисков. Состав и степень детализации событий, происходящих в ИС налоговых органов, определяется принятым уровнем допустимого риска. Для оценки информационных рисков в ИС налоговых органов необходимо:

идентифицировать прикладные и обеспечивающие процессы, проходящие в ИС налоговых органов, влияющие на информационный риск, оценить степень их критичности;

оценить накопленный мировой опыт взлома распределенных вычислительных систем, злоупотреблений и частоты, использования имеющих место уязвимостей;

определить степень взаимодействия технических средств обработки информации ИС налоговых органов с другими менее защищенными или незащищенными ИС, особенно с внешними;

оценить уровень защищенности прикладных и обеспечивающих процессов ИС налоговых органов, на основе используемых мер и средств защиты.

9.2. Контроль состояния обеспечения безопасности информации

Контроль состояния обеспечения безопасности информации в ходе эксплуатации объектов информатизации налоговых органов проводится с определенной периодичностью, с целью подтверждения состояния обеспечения ИБ и проверки выполнения пользователями ИС налоговых

органов и ответственными лицами структурных подразделений ФНС России исполнения положений Политики ИБ ФНС России и установленного режима защиты ИР ФНС России. Контроль проводится также в случаях нарушения ИБ с целью определения причин произошедших нарушений.

Контроль состояния обеспечения безопасности информации в ходе эксплуатации объектов информатизации налоговых органов проводится специалистами подразделений информационной безопасности центрального аппарата ФНС России и территориальных налоговых органов, в плановом порядке или вне плана, в случаях нарушения безопасности информации с целью определения причин произошедших нарушений.

Для проведения контроля могут привлекаться организации, имеющие лицензию ФСТЭК России на осуществление такой деятельности.

Контроль состояния обеспечения безопасности информации, содержащей сведения, составляющие государственную тайну, или в КСИИ осуществляют представители ФСТЭК России, а если при этом применяются средства криптографической защиты информации, органы ФСБ России. Проверки носят плановый характер и согласовываются центральным аппаратом ФНС России с контролирующими органами.

Основными задачами контроля являются:

проверка соответствия организации работ по обеспечению ИБ в налоговых органах требованиям установленного режима защиты ИР ФНС России;

проверка соответствия ИС налоговых органов установленному уровню защищенности;

оценка обоснованности мер ИБ, применяемых в налоговых органах и соответствия их установленным требованиям;

проверка своевременности и полноты выполнения сотрудниками ФНС России требований нормативных документов по обеспечению безопасности информации, в том числе положений настоящей Концепции.

В ходе контроля состояния обеспечения безопасности информации могут применяться специальные программные средства тестирования технических средств обработки информации. Тестовые испытания состояния безопасности информации проводятся в рабочих эксплуатационных режимах ИС налоговых органов. При проведении контроля необходимо учитывать, что использование тестирующих средств не достаточно для объективного контроля защищенности ИС налоговых органов. Перечень выявленных при тестировании уязвимостей не является исчерпывающим и не исключают присутствия иных, кроме обнаруженных уязвимостей. Результаты испытаний с помощью тестирующих средств подлежат обязательному дополнению результатами других исследований. Тестированию подвергаются:

встроенные механизмы защиты общесистемного программного обеспечения ИС налоговых органов и телекоммуникационного оборудования;

программные и программно-аппаратные средства защиты, применяемые в ИС налоговых органов;

технические СЗИ, установленные на объектах информатизации налоговых органов;

основные технические средства обработки информации ИС налоговых органов и телекоммуникационной инфраструктуры ФНС России;

вспомогательные технические средства обработки информации, установленные на объектах информатизации налоговых органов.

По результатам контроля даётся оценка эффективности, принимаемых мер обеспечения безопасности информации. Защита считается эффективной, если принимаемые меры обеспечивают реализацию заданных целей и требований, а также соответствуют установленным нормам и требованиям настоящей Концепции.

Результаты контроля, установленные причины нарушений, рекомендации по их устранению отражаются в заключениях, актах, справках или отчетах, и докладываются Руководителю Федеральной налоговой службы.

9.3. Аудит (обследование) обеспечения безопасности информации

Аудит (обследование) обеспечения безопасности информации на объектах налоговых органов проводится сторонними организациями, имеющими опыт проведения аудита безопасности информации (исполнителями аудита). Аудит проводится по инициативе руководства ФНС России. Поддержка руководством ФНС России является необходимым условием для проведения аудита.

Аудит (обследование) представляет собой комплекс мероприятий, в которых помимо аудитора, задействованы сотрудники структурных подразделений ФНС России. Действия всех участников этого процесса должны быть скоординированы.

На этапе инициирования процедуры аудита (обследования) должны быть решены следующие организационные вопросы:

права и обязанности аудитора должны быть четко определены и документально закреплены;

аудитором должен быть подготовлен и согласован с руководством ФНС России план проведения аудита;

руководством ФНС России должны быть определены общие границы объекта обследования (аудита);

аудитором совместно с руководством ФНС России должен быть произведен выбор критериев оценки состояния ИБ;

сотрудники ФНС России должны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

Объектами аудита (обследования) в ФНС России могут быть:

организационно-распорядительная, эксплуатационная и конструкторская документация, регламентирующая организацию и порядок обеспечения ИБ в ФНС России;

ИС налоговых органов и телекоммуникационная инфраструктура ФНС России;

сотрудники ФНС России, привлекаемые к обработке защищаемых ИР ФНС России и обслуживанию технических средств обработки информации налоговых органов.

При определении границ объекта аудита (обследования) должны быть четко зафиксированы:

территориальное расположение обследуемого объекта и его частей (подразделений налоговых органов);

точки разграничения ответственности с провайдерами телематических услуг при передаче информации между удаленными элементами ИС и объектами информатизации налоговых органов;

разграничение ответственности по обслуживанию коммуникационного оборудования телекоммуникационной инфраструктуры ФНС России;

разграничение ответственности в обеспечении физической охраны объектов информатизации налоговых органов.

Для решения конкретных задач аудита (обследования) применяются специальные методики и установленные критерии. В качестве критериев оценки определяются стандарты (национальные и международные), либо требования ФНС России.

Программа аудита (обследования), должна предусматривать (не ограничиваясь):

анализ документов по использованию ИС налоговых органов и обеспечению ИБ в ФНС России;

анализ структуры, состава и принципов работы ИС налоговых органов и существующей СиЗИ;

оценка порядка и правильности классификации ИР ФНС России, определение (уточнение) требуемого уровня защищенности ИС налоговых органов;

анализ деятельности должностных лиц и сотрудников ФНС России по обеспечению ИБ;

оценка подготовки сотрудников ФНС России к поддержанию установленного режима защиты ИР ФНС России;

оценка порядка и достаточности администрирования ИС налоговых органов и управления доступом к ИР ФНС России;

оценка (тестовые испытания) эффективности существующей СиЗИ ИС налоговых органов;

оценка обеспечения безопасности сотрудников ФНС России и физической безопасности объектов информатизации налоговых органов;

оценка достаточности планирования бесперебойной работы ИС налоговых органов;

проведение проверки выполнения установленных правил (политики) ИБ, порядка применения СЗИ, порядка копирования защищаемого авторским правом программного обеспечения, порядка уведомления о случаях нарушения защиты информации.

Результатом проведения аудита (обследования) является отчёт о состоянии защищенности ИС налоговых органов, в котором на основе анализа достигнутого уровня и динамики развития информационных технологий, ожидаемых угроз, источников этих угроз и уязвимостей (факторов), даются развернутые рекомендации по повышению уровня защищенности ИС налоговых органов, на основе совершенствования механизмов (исполнительных и поддержки) СОБИ ФНС России.

В ходе аудита (обследования) анализируется возможность причинения ущерба интересам субъектов правоотношений при активизации возможных уязвимостей ИС налоговых органов.

_____

* Р 50.1.053-2005. Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации

Приложение № 1

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

См. графический объект

“Рис. 1. Обобщенная структура защищаемых информационных ресурсов ФНС России”

1.png

Рис. 1. Обобщенная структура защищаемых информационных ресурсов ФНС России

См. графический объект

“Рис. 2. Модель реализации угроз безопасности”

2.png

Рис. 2. Модель реализации угроз безопасности

См. графический объект

“Рис. 3. Взаимосвязь направлений сохранения свойств информации и угроз безопасности”

3.png

Рис. 3. Взаимосвязь направлений сохранения свойств информации и угроз безопасности

См. графический объект

“Рис. 4. Структура СОБИ ФНС России”

4.png

Рис. 4. Структура СОБИ ФНС России

См. графический объект

“Рис. 5. Содержание задач на различных уровнях СОБИ ФНС России”

5.png

Рис. 5. Содержание задач на различных уровнях СОБИ ФНС России

См. графический объект

“Рис. 6. Задачи, решаемые исполнительным механизмом СОБИ ФНС России”

6.png

Рис. 6. Задачи, решаемые исполнительным механизмом СОБИ ФНС России

См. графический объект

“Рис. 7. Задачи, решаемые механизмом поддержки СОБИ ФНС России”

7.png

Рис. 7. Задачи, решаемые механизмом поддержки СОБИ ФНС России

См. графический объект

“Рис. 8. Принцип системы управления информационной безопасностью ФНС России”

8.png

Рис. 8. Принцип системы управления информационной безопасностью ФНС России

См. графический объект

“Рис. 9. Задачи СУИБ на разных уровнях СОБИ ФНС России”

9.png

Рис. 9. Задачи СУИБ на разных уровнях СОБИ ФНС России

См. графический объект

“Рис. 10. Общая архитектура организационной базы по уровням СОБИ и их взаимосвязь”

10.png

Рис. 10. Общая архитектура организационной базы по уровням СОБИ и их взаимосвязь

См. графический объект

“Рис. 11. Укрупненная структура Политики безопасности информации ФНС России”

11.png

Рис. 11. Укрупненная структура Политики безопасности информации ФНС России

См. графический объект

“Рис. 12. Взаимосвязь подуровней исполнительного механизма и функциональных контуров СиЗИ”

12.png

Рис. 12. Взаимосвязь подуровней исполнительного механизма и функциональных контуров СиЗИ

IDS - средства обнаружения вторжений

IPS - средства предотвращения вторжений

AVP - средства антивирусной защита

CF - средства контроля содержимого передаваемых данных

VPN - средства создания виртуальных частных защищенных сетей

ЭЦП - средства формирования электронной подписи

МЭ - средства межсетевого экранирования

См. графический объект

“Рис. 13. Взаимосвязь слоев и функциональных компонент механизма поддержки СОБИ”

13.png

Рис. 13. Взаимосвязь слоев и функциональных компонент механизма поддержки СОБИ

Приложение № 2

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Рекомендации

по порядку применения положений Концепции в деятельности должностных лиц и работников ФНС России

1. Разработка документов Политики информационной безопасности ФНС России

Единая Политика информационной безопасности ФНС России (см. IV.3.1) представляет собой совокупность взаимоувязанных нормативных и организационно-распорядительных документов ФНС России. Разработка организационно-распорядительных документов проводится после уяснения цели (см. I.4) и задач (см. I.5) ИБ ФНС России, сформулированных в настоящей Концепции, правомочий субъектов (см. III, IV) информационных отношений и объектов защиты (см. II), структуры политики ИБ ФНС России (см. IV.3.1), направленности деятельности налоговых органов (см. I.6), принципов построения СОБИ (см. Приложение 6). Для подготовки организационно-распорядительных документов Политики информационной безопасности ФНС России необходимо:

По-видимому, в тексте предыдущего абзаца допущена опечатка. Вместо слов “см. IV.3.1” следует читать “см. VI.3.1”

уяснить на основе стоящих целей и задач (см. I.4, I.5) какие вопросы информационной безопасности ФНС России подлежат регулированию предполагаемым к разработке организационно-распорядительным документом;

определить (см. Приложение 1 рис. 7) к какому уровню СОБИ относятся вопросы ИБ, подлежащие регулированию предполагаемым к разработке организационно-распорядительным документом, с учетом правомочий субъектов информационных отношений (см. III, IV) к чьей компетенции относится вопрос, подлежащий регулированию;

выбрать, исходя из выбранного уровня СОБИ, тип организационно-распорядительного документа (см. рис. 10), подлежащего к разработке и необходимого для регулирования предполагаемого вопроса ИБ ФНС России;

ознакомиться с «Примерным перечнем организационно-распорядительных документов, которые необходимо разработать в ФНС России» (см. Приложение 7) и уточнить какие из уже разработанных организационно-распорядительных документов могут содержать нормы, затрагивающие область регулирования отношений, предполагаемого к решению вопроса;

сформулировать с учетом принципов построения СОБИ (см. Приложение 6), состав мер (см. Приложение 10) и мероприятий (см. Приложение 10), подлежащих реализации, имеющихся организационно-распорядительных документов ФНС России, необходимые для регулирования отношений при решении вопроса нормы и составить проект организационно-распорядительного или нормативного документа;

при наличии в ФНС России организационно-распорядительного документа Политики информационной безопасности ФНС России, регулирующего аналогичные или смежные вопросы, оценить необходимость внесения изменений в действующие документы и подготовить такие изменения;

определить (при необходимости) состав дополнительных документов более низкого уровня, которые необходимо разработать в развитие положений проекта организационно-распорядительного документа по вопросу, требующему регулирования.

2. Выработка ответственными лицами взаимосвязанных и согласованных мер защиты

Выработка ответственными лицами взаимосвязанных и согласованных мер защиты предполагает предварительное изучение положений настоящей Концепции с целью уяснения цели (см. I.4) и задачи (см. I. 5) информационной безопасности ФНС России, объектов защиты (см. II), субъектов отношений (см. III), принципов построения СОБИ (см. Приложение 6), направленности деятельности налоговых органов (см. I.6), состава мер (см. Приложение 9) и мероприятий (см. Приложение 10), подлежащих исполнению, основ построения и архитектуры СОБИ (см. IV.3) и особенностей обеспечения информационной безопасности в различных ситуациях (см. VIII.). При выработке согласованных мер необходимо:

сформулировать вопрос, который необходимо решить мерами защиты, определить объекты, подлежащие защите (см. II) и оценить возможные угрозы (см. V.);

определить на основе анализа актуальных угроз (см. Приложение 4), с учетом возможных последствий, возможные объекты воздействия и актуальные источники угроз, сформулировать необходимые меры защиты;

определить исходя из архитектуры СОБИ (см. IV.3.) и задач, стоящих перед исполнительским механизмом и механизмом поддержки к каком подуровню СОБИ относятся предполагаемые к реализации меры защиты;

определить исходя из установленных подуровней исполнительского уровня СОБИ состав функций защиты (см. Приложение 8, Приложение 11), необходимых для реализации на выбранном подуровне, уяснить какие из необходимых мер уже реализованы механизмами защиты СОБИ, какими мерами, возможно, реализовать недостающие функции безопасности, уточнить формулировки мер защиты;

определить исходя из архитектуры организационной базы СОБИ (см. IV.3.1, Приложение 1 рис. 8) какие подразделения ФНС России необходимо задействовать при реализации предполагаемых мер защиты, определить границы их ответственности;

По-видимому, в тексте предыдущего абзаца допущена опечатка. Вместо слов “см. IV.3.1” следует читать “см. VI.3.1”

сформулировать на основе полученных сведений задания соответствующим подразделениям ФНС России по реализации мер защиты и оформить соответствующие распоряжения.

3. Принятие должностными лицами ФНС России управленческих решений

Принятие должностными лицами управленческих решений по реализации выработанной Политики обеспечения информационной безопасности ФНС России осуществляется на основе глубокого уяснения цели (см. I.4) и задач (см. I.5) информационной безопасности ФНС России, сформулированных в настоящей Концепции, правомочий субъектов (см. III) информационных отношений и объектов защиты (см. II), структуры политики информационной безопасности ФНС России, направленности деятельности налоговых органов, принципов построения СОБИ (см. Приложение 6), требований, предъявляемых к СОБИ (см. VII) и особенностей обеспечения информационной безопасности в различных ситуациях (см. VIII), а также детального изучения имеющихся организационно-распорядительных документов Политики информационной безопасности ФНС России. При принятии управленческих решений необходимо:

сформулировать на основе стоящих целей и задач информационной безопасности ФНС России (см. I.4, I.5) и разработанных организационно-распорядительных документов Политики информационной безопасности ФНС России, вопрос, требующий принятия управленческого решения;

уяснить (см. рис. 5), к какому уровню СОБИ относятся вопросы информационной безопасности, требующие принятия управленческого решения, определить к чьей компетенции относится принятие управленческого решения;

принять исходя из стоящих задач управленческое решение, при необходимости внести изменения в должностные инструкции сотрудников ФНС России, направленные на исполнение принятого управленческого решения;

организовать исполнение принятого управленческого решения и контроль за его исполнением (см. IX).

4. Определение ролей и ответственности должностных лиц и работников ФНС России

Определение ролей и ответственности должностных лиц и работников ФНС России в сфере обеспечения безопасности информации осуществляется на основе изучения содержания и структуры Политики информационной безопасности ФНС России (см. VI.3.1), действующих организационно-распорядительных документов Политики ФНС России (см. Приложение 7), структуры организационной базы СОБИ ФНС России (см. VI.2.3), требований к СОБИ ФНС России (см. VII). При определении ролей и ответственности должностных лиц и работников ФНС России необходимо:

установить категорию работников ФНС России, которым необходимо определить роли и ответственность в сфере обеспечения информационной безопасности;

уяснить место работника в составе организационной базы СОБИ ФНС России (см. VI.3.1) и состав организационно-распорядительных документов исполнительского уровня Политики информационной безопасности ФНС России, регулирующих ответственность данного работника (Приложение 7);

уяснить на основе изучения организационно-распорядительных документов исполнительского уровня Политики информационной безопасности ФНС России, требования к исполнительскому уровню СОБИ (см. VII), правомочия субъектов информационных отношений (см. IV.), задачи информационной безопасности ФНС России, рекомендации по формированию организационной базы (см. VI.2.3), роли работников ФНС России;

разработать на основе полученных знаний обязанности работников ФНС России в сфере информационной безопасности;

установить роль работников ФНС России в общей структуре организационной базы СОБИ ФНС России;

определить работников ФНС России, обладающих полномочиями в решении вопросов информационной безопасности;

установить ответственность сотрудников ФНС России при решении вопросов информационной безопасности;

закрепить роль, обязанности, полномочия, ответственность работников ФНС России в должностных регламентах и организационно-распорядительных документах в сфере информационной безопасности ФНС России второго и третьего (оперативного) уровня Политики информационной безопасности ФНС России.

5. Разработка технических заданий на создание (модернизацию) объектов информатизации

При разработке технических заданий на создание (модернизацию) объектов информатизации налоговых органов необходимо предъявлять требования по информационной безопасности и защите информации. Разработка технических заданий (частных технических заданий) требует глубокого изучения состава объектов защиты (см. II), угроз информационной безопасности (см. V.1) возможностей нарушителей (см. V.2), архитектуры СОБИ ФНС России (см. VI.2, VI.3), требований к исполнительному механизму СОБИ ФНС России, реализуемому СиЗИ (Приложение 8) и особенностей обеспечения ИБ в различных ситуациях (см. VIII), а также организационно-распорядительных документов Политики информационной безопасности ФНС России оперативного уровня и нормативных документов федеральных органов государственной власти, уполномоченных в обеспечении ИБ. При разработке технических заданий на создание (модернизацию) объектов информатизации налоговых органов необходимо:

уяснить требования базового уровня защищенности ИС налоговых органов (см. VII.1.2);

определить необходимость уточнения требований базового уровня и провести его уточнение с учетом требований руководящих документов ФСТЭК России и ФСБ России (при необходимости);

определить к какому функциональному контуру СиЗИ (исполнительного механизма СОБИ ФНС России) и подуровню исполнительского уровня СОБИ ФНС России (см. VII.2.2.) относятся проектируемые элементы информационной системы налоговых органов;

определить с учетом выбранного уровня защищенности информационных систем налоговых органов состав функций, которые должны быть реализованы выбранными функциональными контурами исполнительного механизма СОБИ ФНС России (см. Приложение 8);

определить с учетом выбранного уровня защищенности информационных систем налоговых органов состав мероприятий, который должен быть реализован механизмом поддержки на выбранном подуровне исполнительского уровня СОБИ ФНС России (см. Приложение 9, Приложение 10);

определить с учетом выбранного уровня защищенности информационных систем налоговых органов примерный состав средств защиты информации и места их возможного размещения, а также основные требования к ним, позволяющие решить задачи информационной безопасности (см. Приложение 12);

определить необходимость локализации информационных ресурсов ФНС России и выбрать дополнительные требования (см. Приложение 13), необходимость использования СКЗИ и выбрать дополнительные требования (см. VI.2.3, VII.2.4, VII.2.5, VII.2.6);

определить с учетом выбранного уровня защищенности информационных систем налоговых органов на основе организационно-распорядительного документа второго (оперативного) уровня Политики информационной безопасности ФНС России «Общие технические требования по обеспечению безопасности информации при разработке и внедрении прикладных систем ФНС России» и нормативных документов ФСТЭК России и ФСБ России конкретный набор функций безопасности, которые должны быть реализованы средствами защиты информации, входящими в СиЗИ.

Подготовить проект технического задания (частного технического задания на создание элементов) на создание (модернизацию) объектов информатизации налоговых органов.

Приложение № 3

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Перечень

актуальных угроз для объектов ФНС России № п/п Основные источники угроз Угроза Уровень реализации угрозы Объект воздействия Уязвимость Основные последствия (ущерб) для ФНС России и субъектов

1. неблагоприятные события природного характера, в том числе пожары, стихийные бедствия, магнитные бури природные катаклизмы (стихийные) Нарушение доступности, целостности Физический уровень Оборудование АИС (серверы, АРМ, сетевое оборудование) Потенциальная подверженность района размещения объектов АИС воздействию природных катаклизмов (пожары, наводнения и др.) Выход из строя информационно-телекоммуникационной системы (технических средств АИС: серверов, АРМ администраторов и пользователей, коммуникационного и сетевого оборудования), потеря управления, прекращение (отказ) обслуживания, утеря (уничтожение) данных вследствие физического разрушения (порчи) носителей информации

неблагоприятные события техногенного характера, в том числе аварии на средствах инженерных коммуникаций, средствах телекоммуникационной инфраструктуры, сбои и отказы оборудования (техногенные) Подверженность объектов АИС воздействию техногенных факторов: катастроф, аварий, сбоев функционирования систем энергоснабжения, инженерных коммуникаций, связи и др.

Недостаточная катастрофоустойчивость и отказоустойчивость аппаратно-программных и технических комплексов

2. иностранные технические разведки (ИТР) (антропогенные, внешние) Нарушение доступности, целостности, конфиденциальности Физический уровень Оборудование АИС (серверы, АРМ, сетевое оборудование) Побочные электромагнитные излучения (ПЭМИН) электронно-вычислительной техники, акустические и видовые разведки. Деструктивные информационные воздействия на информацию Утечка информации, ее уничтожение и блокирование.

Нарушение доступности, целостности

Нарушение доступности, целостности, конфиденциальности Сетевой уровень Маршрутизаторы коммутаторы, концентраторы Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки воздействия ИТР Выход из строя информационно-телекоммуникационной системы, потеря управления, прекращение

(отказ) обслуживания, утеря (уничтожение) данных в следствии физического разрушения (порчи) носителей информации

3 террористы, криминальные элементы (антропогенные, внешние) Нарушение доступности, целостности, конфиденциальности Физический уровень Оборудование АИС (серверы, АРМ, сетевое оборудование) Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия Выход из строя информационно-телекоммуникационной системы, потеря управления, прекращение (отказ) обслуживания, утеря (уничтожение) данных в следствии физического разрушения (порчи) носителей информации

Нарушение доступности, целостности Недостатки в организации охраны и технической укрепленности объектов ФНС России

Нарушение доступности, целостности, конфиденциальности Сетевой уровень Маршрутизаторы коммутаторы, концентраторы Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия Реализация атак (нерегламентированное использование инструментов, позволяющих реализовать атаки) на информационно-телекоммуникационные системы ФНС России приводящие к прекращению (отказу) обслуживания, модификации настроек сетевого оборудования, неправомерному доступу к оборудованию (сегментам сети)

Нарушение доступности, целостности, конфиденциальности Уровень сетевых приложений и сервисов Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы) Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия Реализация атак (нерегламентированное использование инструментов позволяющих реализовать атаки) на информационно-телекоммуникационные системы ФНС России приводящие к прекращению (отказу) обслуживания отдельных сервисов, изменение (модификация) сетевого трафика, перехват информации

Нарушение доступности, целостности, конфиденциальности Уровень операционных систем Файлы данных с защищаемой информацией Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия Внедрение вредоносного программного кода, позволяющего захватить управление операционными системами с целью прекращения (отказа) обслуживания отдельных хостов (групп хостов), изменение (модификация) программного окружения, перехват конфиденциальной информации

Нарушение доступности, целостности, конфиденциальности Уровень систем управления базами данных Базы данных с защищаемой информацией Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия Реализация атак (нерегламентированное использование инструментов, позволяющих реализовать атаки), внедрение вредоносного программного кода, позволяющего захватить управление СУБД с целью прекращения (отказа) обслуживания, модификации информации

Нарушение доступности, целостности, конфиденциальности Уровень технологических процессов и приложений Прикладные программы доступа и обработки информации, АРМ АИС Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия Нарушение непрерывности и правильности функционирования бизнес-процессов. Внедрение фиктивных (подложных) документов. Угроза деловой репутации

4. компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе с использованием компьютерных вирусов и других типов вредоносных кодов (антропогенные, внешние) Нарушение доступности, целостности Сетевой уровень Маршрутизаторы, коммутаторы, концентраторы Восприимчивость программного обеспечения к вирусам и другим атакам Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных.

Нарушение доступности, целостности Наличие уязвимостей программного и аппаратного обеспечения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных

Нарушение доступности, целостности Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Уровень сетевых приложений и сервисов Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы) Восприимчивость программного обеспечения к вирусам и другим атакам Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей программного и аппаратного обеспечения Прекращение (отказа) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных

атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказа) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Уровень операционных систем Файлы данных с защищаемой информацией (защищаемые ИР ФНС России) Восприимчивость программного обеспечения к вирусам и другим атакам Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей программного и аппаратного обеспечения Прекращение (отказа) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Несоответствующая утвержденной

документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Уровень систем управления базами данных Базы данных с защищаемой информацией (защищаемые ИР ФНС России) Восприимчивость программного обеспечения к вирусам и другим атакам Прекращение (отказа) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей программного и аппаратного обеспечения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Уровень технологических процессов и приложений Прикладные программы доступа и обработки информации, рабочие станции пользователей (АРМ) информационных систем налоговых органов Восприимчивость программного обеспечения к вирусам и другим атакам Прекращение (отказа) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей (дыр) программного и аппаратного обеспечения, в том числе наличие в нем недекларированных возможностей Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети)

Нарушение доступности, целостности, конфиденциальности Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, отвлечение персонала на ликвидацию последствий вирусных атак, потеря (модификация) данных, неправомерный доступ к информационным ресурсам (оборудованию, сегментам сети).

5. поставщики программно-технических средств, расходных материалов, услуг, в том числе провайдеры телематических услуг (антропогенные, внешние) подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования информационных систем налоговых органов и его ремонт (антропогенные, внешние) Нарушение доступности, целостности Физический уровень Оборудование информационных систем налоговых органов (серверы, АРМ, сетевое оборудование) Некачественная (неполная) регламентация в договорах вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность) Отказ поставщика

предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств

Нарушение доступности, целостности Ориентация на монопольных поставщиков и подрядчиков Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств

Нарушение доступности, целостности, конфиденциальности Сетевой уровень Маршрутизаторы, коммутаторы, концентраторы телекоммуникационной инфраструктуры ФНС России Некачественная (неполная) регламентация в договорах вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств

Нарушение доступности, целостности, конфиденциальности Ориентация на монопольных поставщиков и подрядчиков Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств

Нарушение доступности, целостности, конфиденциальности Уровень сетевых приложений и сервисов Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы) Некачественная (неполная) регламентация в договорах вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность) Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств

Нарушение доступности, целостности, конфиденциальности Ориентация на монопольных поставщиков и подрядчиков Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств

Нарушение доступности, целостности, конфиденциальности Уровень операционных систем Файлы данных с защищаемой информацией (защищаемые ИР ФНС России) Некачественная (неполная) регламентация в договорах вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность) Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживания в следствие выхода из строя аппаратных и/или программных средств. Внедрение вредоносного программного обеспечения.

Нарушение доступности, целостности, конфиденциальности Ориентация на монопольных поставщиков и подрядчиков Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживания вследствие выхода из строя аппаратных и/или программных средств. Внедрение вредоносного программного обеспечения.

Нарушение доступности, целостности, конфиденциальности Уровень систем управления базами данных Базы данных с защищаемой информацией (защищаемые ИР ФНС России) Некачественная (неполная) регламентация в договорах вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность) Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств. Внедрение вредоносного программного обеспечения. Неправомерный доступ к информации.

Нарушение доступности, целостности, конфиденциальности Ориентация на монопольных поставщиков и подрядчиков Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание вследствие выхода из строя аппаратных и/или программных средств. Внедрение вредоносного программного обеспечения. Неправомерный доступ к информации.

Нарушение доступности, целостности, конфиденциальности Уровень технологических процессов и приложений Прикладные программы доступа и обработки информации, рабочие станции пользователей (АРМ) информационных систем налоговых органов Некачественная (неполная) регламентация в договорах вопросов взаимодействия с поставщиками и подрядчиками (обязанности, ответственность) Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание в следствии выхода из строя аппаратных и/или программных средств. Внедрение вредоносного программного обеспечения. Неправомерный доступ к информации. Нарушение требований конфиденциальности, утечка данных.

Нарушение доступности, целостности, конфиденциальности Ориентация на монопольных поставщиков и подрядчиков Отказ поставщика предоставить гарантийное (послегарантийное) сопровождение и как следствие прекращение (отказ) обслуживание вследствие выхода из строя аппаратных и/или программных средств. Внедрение вредоносного программного обеспечения. Неправомерный доступ к информации. Нарушение требований конфиденциальности, утечка данных.

6. сотрудники налоговых органов, являющиеся легальными участниками процессов обработки информации и действующие вне рамок предоставленных полномочий (антропогенные, внутренние) Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Физический уровень Оборудование информационных систем налоговых органов (серверы, АРМ, сетевое оборудование) Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, потеря данных вследствие физического воздействия на информационно-телекоммуникационные системы ФНС России

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Сетевой уровень Маршрутизаторы, коммутаторы, концентраторы телекоммуникационной инфраструктуры ФНС России Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, модификация настроек сетевого оборудования, неправомерный доступ к сетевому оборудованию (сегменту сети)

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень сетевых приложений и сервисов Программные

компоненты передачи данных по компьютерным сетям (сетевые сервисы) Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания конкретных сервисов, модификация настроек сетевого оборудования, неправомерный доступ к сетевому оборудованию (сегменту сети)

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень операционных систем Файлы данных с защищаемой информацией (защищаемые ИР ФНС России) Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, модификация настроек (внедрение вредоносных программ), неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, модификация настроек (внедрение вредоносных программ), неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень систем управления базами данных Базы данных с защищаемой информацией (защищаемые ИР ФНС России) Наличие уязвимостей (слабостей) в

системе защиты информации Прекращение (отказ) обслуживания СУБД, модификация настроек СУБД, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания СУБД, модификация настроек СУБД, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания СУБД, модификация настроек СУБД, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень технологических процессов и приложений Прикладные программы доступа и обработки информации, рабочие станции пользователей (АРМ) информационных систем налоговых органов Наличие уязвимостей (слабостей) в системе защиты информации Прекращение (отказ) обслуживания, модификация настроек оборудования и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам, внедрение фиктивных (подложных) документов

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания, модификация настроек оборудования и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам, внедрение фиктивных (подложных) документов

7. сотрудники налоговых органов, являющиеся легальными участниками процессов обработки информации и действующие в рамках предоставленных полномочий (антропогенные, внутренние)

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Физический уровень Оборудование информационных систем налоговых органов (серверы, АРМ, сетевое оборудование) Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания, потеря (уничтожение) информации

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Сетевой уровень Маршрутизаторы, коммутаторы, концентраторы телекоммуникационной инфраструктуры ФНС России Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания, модификация настроек сетевого оборудования, неправомерный доступ к сетевому оборудованию (сегменту сети)

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень сетевых приложений и сервисов Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы) Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания конкретных сервисов, модификация настроек оборудования и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания конкретных

сервисов, модификация настроек оборудования и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень операционных систем Файлы данных с защищаемой информацией (защищаемые ИР ФНС России) Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания, модификация настроек оборудования и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания, модификация настроек оборудования и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень систем управления базами данных Базы данных с защищаемой информацией (защищаемые ИР ФНС России) Несоответствие регламентов деятельности текущему состоянию объекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания СУБД, модификация настроек СУБД и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам, внедрение фиктивных (подложных) документов, утечка информации

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения Прекращение (отказ) обслуживания СУБД, модификация настроек СУБД и программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам, внедрение фиктивных (подложных) документов, утечка информации

Нарушение доступности, целостности, конфиденциальности, нарушение регламентов технологических процессов Уровень технологических процессов и приложений Прикладные программы доступа и обработки информации, рабочие станции пользователей (АРМ) информационных систем налоговых органов Несоответствие регламентов для проекта и неконтролируемость исполнения сотрудниками ФНС России регламентов своей деятельности Прекращение (отказ) обслуживания, модификации программных комплексов, внедрение вредоносных программ, неправомерный доступ к информационным ресурсам, внедрение фиктивных (подложных) документов утечка информации

Приложение № 4

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Общая классификация методов реализации угроз ИБ в ФНС России

Методы реализации делятся на группы по способам реализации. Понятие «метод», применимо только при рассмотрении реализации угроз антропогенными источниками. Для техногенных и стихийных источников, это понятие трансформируется в понятие «предпосылка» Методы реализации угроз Возможные последствия реализации методов

Аналитические методы

Активные аналитические методы

опрос в ходе публичных мероприятий (конференции и пр.) Нарушение конфиденциальности путем прямого получения конфиденциальной информации

опрос бывших (уволенных) сотрудников Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение информации о номерах телефонов, IP адресах пользователей и подсетей, архитектуре сети, открытых серверах, структуре организации и др. информации для дальнейшей реализации угроз

проведение мнимых переговоров Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение информации о номерах телефонов, IP адресах, архитектуре сети, открытых серверах, структуре организации и др. информации для дальнейшей реализации угроз

сканирование и инвентаризация ИС Определение функций ИС, способа представления информации, типа и параметров и версий ПО, носителей информации, идентификация СВТ, СЗИ, идентификация учетных записей пользователей, используемых сервисов и служб, поиск совместно используемых ресурсов, открытых портов, незашифрованных паролей для дальнейшей реализации угроз

Пассивные аналитические методы

анализ информации из СМИ, глобальных ИС, выступлений Получение информации о номерах телефонов, IP адресах пользователей и подсетей, архитектуре сети, открытых серверах, структуре

организации, дефектах ПО, оборудования, нарушениях при эксплуатации оборудования, инструментарии для дальнейшей реализации угроз.

агрегирование и инференция открытой информации Нарушение конфиденциальности путем прямого получения конфиденциальной информации.

Технические методы

Активные технические методы

мониторинг (наблюдение) активности каналов связи Получение информации о номерах телефонов, IP адресах пользователей и подсетей, архитектуре сети, открытых серверах, структуре организации, выявление наиболее уязвимых мест сети для дальнейшей реализации угроз.

радиационное и ионизирующее воздействие Нарушение целостности и доступности информации при передаче по каналам связи, нарушение нормальной работы технических устройств, носителей информации.

электромагнитное воздействие Нарушение целостности и доступности информации при передаче по каналам связи, нарушение нормальной работы технических устройств, носителей информации.

создание условий для сбоев и отказов оборудования и ПО Нарушение целостности и доступности информации при передаче по каналам связи, нарушение нормальной работы технических устройств, носителей информации.

Пассивные технические методы

визуально-оптическое наблюдение и фотографирование Нарушение конфиденциальности путем прямого получение информации ограниченного доступа.

перехват акустических и виброакустических сигналов Нарушение конфиденциальности путем прямого получение информации ограниченного доступа

перехват информации по каналам ПЭМИН Нарушение конфиденциальности путем снятия информационного сигнала по каналу ПЭМИН и получение информации ограниченного доступа

перехват информации в кабельных линиях связи Нарушение конфиденциальности путем прямого получение информации ограниченного доступа.

Программно-аппаратные методы

Активные программно-аппаратные методы

внедрение дезинформации Нарушение целостности и доступности путем введения ложной информации в базы данных и информационные ресурсы, перегрузки системных ресурсов, каналов связи.

загрузка нештатной ОС и ПО Создание условий для дальнейшей реализации угроз, отключение механизмов защиты.

изменение конфигурации ИС и используемых сервисов Отключение механизмов защиты, изменение полномочий пользователей отключение/включение сервисов, перенаправление информации, введение запрета на использование информации для дальнейшей реализации угроз.

маскировка под авторизованного пользователя (маскарад) Нарушение конфиденциальности и целостности путем использования полномочий авторизованных пользователей по чтению и изменению информации.

модификация информации (данных) Нарушение целостности путем модификации информации в базах данных и информационных ресурсах.

модификация ПО и/или его настроек Создание условий дальнейшей реализации угроз.

несанкционированное изменение полномочий Нарушение конфиденциальности и целостности путем изменения (превышения) полномочий авторизованных пользователей по чтению и изменению информации.

перехват управления соединениями Нарушение доступности и конфиденциальности путем стороннего управления активным сеансом.

перехват управления ИС Нарушение конфиденциальности, целостности и доступности путем уничтожения, модификации информации, перегрузки системных ресурсов, нарушения нормальной работы

применение вредоносных программ Нарушение конфиденциальности, целостности и доступности путем уничтожения, модификации информации, перезагрузки системных ресурсов, нарушения нормальной работы технических средств и ПО, физического разрушения технических средств и носителей информации, влияния на персонал ИС, накопления и перенаправления информации по скрытым каналам, введения запрета на использование информации, монопольный захват системных ресурсов.

применение отладочных режимов ИС Создание предпосылок и условий дальнейшей реализации угроз, отключение механизмов защиты.

сканирование и модификация журналов регистрации Сокрытие следов несанкционированных действий после реализации угроз.

интенсивное обращение к ИС и каналам связи Нарушение доступности путем перегрузки сетевых ресурсов и каналов связи.

Пассивные программно-аппаратные методы

наблюдение за активностью работы в ИС Определение функций ИС, способа представления информации, идентификация учетных записей пользователей, используемых сервисов и служб, незашифрованных паролей для дальнейшей реализации угроз.

установка нештатного оборудования или ПО Создание предпосылок и условий дальнейшей реализации угроз.

чтение, копирование информации Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение паролей доступа, списков управления доступом, таблиц маршрутизации, информации о номерах телефонов и IP адресах, архитектуре сети, структуре организации для дальнейшей реализации угроз.

Социальные методы

Активные социальные методы

вербовка, подкуп или шантаж персонала Нарушение конфиденциальности, целостности и доступности путем прямого получения конфиденциальной информации (данных), склонения к уничтожению, модификации информации, ПО. Получение информации о номерах телефонов и IP пользователей, адресах подсетей, архитектуре сети, открытых серверах, структуре организации, дефектах ПО, оборудования, нарушениях при эксплуатации оборудования, инструментарии для дальнейшей реализации угроз.

вхождение в доверие Нарушение конфиденциальности путем прямого получения конфиденциальной информации. Получение информации о номерах телефонов и IP пользователей, адресах подсетей, архитектуре сети, открытых серверах, структуре организации, дефектах ПО, оборудования, нарушениях при эксплуатации оборудования, инструментарии для дальнейшей реализации угроз.

разжигание вражды Создание предпосылок и условий для дальнейшей реализации угроз.

террористические методы (поджег, взрыв, уничтожение) Нарушение целостности и доступности путем уничтожения технических средств, носителей информации, ПО, каналов и линий связи.

Организационные методы

Активные организационные методы

доступ к носителям информации, техническим средствам Нарушение конфиденциальности, целостности и доступности путем получения носителей информации, уничтожения технических средств и носителей информации, модификации информации, ПО.

подделка документов Создание предпосылок и условий для дальнейшей реализации угроз.

разрушение коммуникаций Нарушение целостности и доступности путем нарушения нормальной работы технических средств, каналов и линий связи.

Приложение № 5

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Содержание основных методов противодействия угрозам ИБ

1. Правовые методы

Правовые методы направлены на создание защитного иммунитета, основанного на угрозе применения репрессивных мер в случае нарушения интересов ФНС России или других субъектов и установление механизмов применения определенных санкций в отношении нарушителей. Правовые методы, в основном, ориентированы на устранение угроз, реализуемых источниками антропогенного характера и являются базисом для реализации всех остальных методов защиты. Основными правовыми методами являются:

установление условий и порядка использования и защиты информации;

вменение в обязанность сотрудников налоговых органов и сторонних организаций необходимости сохранения конфиденциальной информации, ставшей им известной в силу служебных обязанностей;

признание права обладания информацией;

введение санкций за противоправные деяния при обращении с информацией;

признание права судебной защиты интересов собственника.

Имеющаяся нормативная правовая база позволяет успешно применять все предусмотренные законом способы защиты гражданских прав для защиты интересов ФНС России в информационной сфере. Законодательством предусмотрена ответственность (в том числе материальная) организаций за правонарушения при использовании защищаемой информации или за несоблюдение режима её защиты. Факт совершения неправомерного действия по получению или завладению информацией, если в отношении неё установлен режим защиты, похищения документов, содержащих такую информацию, подкупа с этой целью сотрудников ФНС России или иного деяния, даже если не наступили какие-либо последствия, расценивается как преступление.

Правовые методы реализуются в ходе совершенствования существующей нормативной правовой базы и способствуют созданию структуры управления обеспечением безопасности информации, координации деятельности и взаимодействия структурных подразделений налоговых органов.

2. Экономические методы

Экономические методы воздействуют на антропогенные источники угроз. В совокупности с правовыми методами направлены на сокращение антропогенных источников угроз и введение в действие механизмов ликвидации последствий реализации угроз.

Основными экономическими методами являются:

введение системы коэффициентов и надбавок;

страхование средств обработки информации;

страхование информационных рисков;

введение механизма возмещения убытков и компенсации ущерба.

Система коэффициентов и надбавок предполагает создание особых льгот работникам ФНС России, работающим с информацией, и направленных на стабилизацию контингента. Эта система увязывается со стажем работы в ФНС России работников, имеющих доступ к ИР, в том числе причастных к организации и осуществлению мер безопасности информации.

Страхование средств обработки информации предполагает страхование ответственности их производителей, а также организаций, осуществляющих создание ИС ФНС России, монтаж оборудования, предоставление каналов связи (провайдеров) и направлено на компенсацию возможного ущерба ФНС России в результате их некомпетентных действий. Страхование информации (информационных рисков) направлено на компенсацию ущерба ФНС России в результате уничтожения (утраты) ИР ФНС России.

3. Организационные методы

Организационные методы в основном ориентированы на работу с персоналом, выбор местоположения и размещения объектов защиты, организацию систем физической, противопожарной защиты, контроля выполнения принятых мер, возложения персональной ответственности за выполнение мер защиты. Методы применяются для уменьшения числа внутренних антропогенных, техногенных и стихийных источников угроз, а также уменьшения влияния уязвимостей. Как правило, эти методы уже частично реализованы на действующих объектах налоговых органов. Основными организационными методами являются:

выбор местоположения и размещения объекта информатизации;

физическая защита и организация охраны;

ограничение доступа в помещения, в которых установлены технические средства обработки информации;

подбор и работа с персоналом;

организация инструктажа персонала;

организация учета оборудования и носителей;

контроль выполнения требований по защите;

противопожарная охрана;

обеспечение надежного сервисного обслуживания;

организация взаимодействия с компетентными органами.

Организационные методы направлены на формирование организационного базиса СОБИ, комплектование налоговых органов специалистами по защите информации, организацию системы общей подготовки кадров, обучение работе с защищаемой информацией и ознакомление персонала с мерами ответственности за неправомерные действия, исключение возможности несанкционированного проникновения на территорию объектов налоговых органов посторонних лиц, обеспечение удобства контроля прохода и перемещения работников ФНС России, создание отдельных зон с самостоятельной системой доступа, контроль за действиями персонала, проведение расследований нарушений установленных правил. Устранение угроз организационными методами является наименее затратным мероприятием по защите информации.

4. Инженерно-технические методы

Инженерно-технические методы ориентированы на оптимальное построение зданий, сооружений, инженерных сетей и транспортных коммуникаций налоговых органов с учетом требований обеспечения безопасности ИР. Эти методы, как правило, реализуются на этапе строительства или реконструкции объектов, способствуют повышению их общей живучести и устраняют источники угроз, обусловленные стихийными бедствиями и факторами техногенного характера, не устранимыми другими методами. Они направлены на ослабление влияния большого количества объективных и случайных уязвимостей. К инженерно-техническим методам относятся:

обеспечение электрозащиты оборудования и зданий;

экранирование помещений;

защита помещений от разрушений;

оптимальное размещение оборудования;

оптимальное размещение инженерных коммуникаций;

применение средств визуальной защиты;

акустическая обработка помещений;

применение систем кондиционирования.

5. Технические методы

Технические методы основаны на применении специальных технических средств защиты информации, контроля обстановки и ориентированы на устранение угроз, связанных с действиями внешних антропогенных источников угроз по воздействию на информацию техническими средствами. Некоторые из этих методов позволяют устранить воздействие техногенных источников угроз и ослабляют влияние объективных, субъективных и случайных уязвимостей. К техническим методам относятся:

резервирование технических средств обработки;

резервирование каналов связи;

использование выделенных каналов связи;

создание резервной копии (дублирование) информационных ресурсов;

создание системы пространственного зашумления;

создание системы акустического и вибрационного зашумления;

экранирование узлов и оборудования;

использование доработанного оборудования;

использование источников гарантированного питания;

контроль каналов связи для передачи информации;

контроль отсутствия электронных устройств перехвата информации на объектах.

6. Программно-аппаратные методы

Программно-аппаратные методы нацелены на устранение проявления угроз, непосредственно связанных с процессом обработки и передачи информации в ИС ФНС России. Без этих методов невозможно построение целостной СОБИ. Содержание программно-аппаратных методов соответствует классам функциональных компонент, приведенных в ГОСТ ИСО/МЭК 15408-2002. Реализация программно-аппаратных методов существенно снижает влияние внутренних антропогенных источников угроз. В этой группе объединяются такие методы, как:

ограничение доступа к средствам обработки (ПО, техническим средствам);

ограничение доступа к объектам защиты (защищаемым информационным ресурсам);

разграничение доступа субъектов (пользователей);

управление внешними потоками информации;

управление внутренними потоками информации;

скрытие структуры и назначения;

подтверждение подлинности информации;

преобразование (шифрование, кодирование) информации при её передаче;

преобразование (шифрование, кодирование) информации при её хранении;

блокирование не используемых сервисов;

мониторинг целостности ПО, конфигурации ПО и аппаратных средств;

мониторинг атак и разрушающих воздействий;

мониторинг действий субъектов.

Приложение № 6

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Основные принципы построения СОБИ ФНС России

1. Принцип законности

Проведение защитных мероприятий, реализуемых СОБИ, должно быть согласовано с требованиями законодательства Российской Федерации в области информации, информационных технологий и

защиты информации, с применением всех дозволенных методов обнаружения и пресечения нарушений при работе с информацией. Принятые меры защиты не должны препятствовать законному доступу граждан и организаций к информации о деятельности ФНС России.

2. Принцип системности и комплексности

Системный подход к построению СОБИ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения задач обеспечения безопасности информационных ресурсов ФНС России. При создании СОБИ должны учитываться все слабые и наиболее уязвимые места объектов информатизации налоговых органов. Комплексное использование методов и средств защиты предполагает их согласованное применение, перекрывающее все существенные (значимые) атаки при реализации актуальных угроз.

3. Принцип максимальной дружественности и прозрачности

Противодействие угрозам информационной безопасности всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу объекта информатизации, так как всегда налагает ограничения организационного и технического характера. СОБИ должна быть максимально совместима с используемыми программной и аппаратной платформами информационных систем налоговых органов и, по возможности, учитывать сложившиеся в них традиции в обмене информационными потоками. Основным назначением информационных систем налоговых органов является обеспечение потребностей пользователей в необходимой информации. Поэтому СОБИ должна работать в «фоновом» режиме и не мешать пользователям в основной работе, но при этом выполнять все возложенные на неё задачи.

4. Принцип превентивности

СОБИ должна быть нацелена прежде всего на недопущение реализации угроз информационной безопасности, а не на устранение последствий их проявления, которое может потребовать значительных финансовых и временных затрат, гораздо больших, чем затрат на создание и поддержание СОБИ.

5. Принцип оптимальности и разумной разнородности

При создании СОБИ должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам информационной безопасности. Согласованное применение разнородных средств при построении целостной системы защиты позволяет устранить слабые места на стыках отдельных компонентов. Средства защиты, используемые СОБИ, должны

дублировать основные функции защиты и быть разных производителей, что позволяет существенно затруднить процесс преодоления защиты за счет различной логики построения средств защиты.

6. Принцип адекватности и непрерывности

Методы защиты должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз информационной безопасности и степени конфиденциальности информации. СОБИ должна реализовывать процесс защиты информации непрерывно и целенаправленно, начиная от стадии проектирования, и на протяжении всего жизненного цикла объектов информатизации налоговых органов.

7. Принцип системного подхода и рациональной этапности

При построении СОБИ должен быть заложен комплекс мероприятий по противодействию угрозам информационной безопасности уже на стадии проектирования (модернизации) объектов информатизации налоговых органов, обеспечивающий оптимальное сочетание комплекса организационных и технических мер защиты информации. При построении СОБИ должно предполагаться первоочередное решение задач создания общей для ФНС России инфраструктуры СОБИ.

8. Принцип адаптивности

СОБИ должна строиться с учетом возможного изменения конфигурации информационных систем налоговых органов, числа пользователей, степени конфиденциальности и ценности информации. При этом введение каждого нового элемента информационной системы или изменение действующих условий не должно снижать достигнутый уровень защищенности в целом.

9. Принцип доказательности и обязательности контроля

При создании СОБИ должны соблюдаться организационные меры защиты, и применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. СОБИ должна обеспечивать обязательность и своевременность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.

10. Принцип самозащиты и конфиденциальности

При построении СОБИ должна соблюдаться конфиденциальность реализованных механизмов защиты информации. Указанный принцип требует реализацию контроля целостности информационных

систем налоговых органов, управления безопасностью через администратора безопасности, реализации возможности восстановления СОБИ при ее компрометации и отказах оборудования.

11. Принцип многоуровневости и равнопрочности

СОБИ должна реализовывать защиту информации на всех уровнях реализации угроз. Защита должна строиться эшелонировано, и иметь несколько последовательных, взаимно перекрывающихся рубежей так, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к реализации угрозы. СОБИ должна обеспечивать возможность сохранения своих защитных функций при изменении конфигурации информационных систем налоговых органов, обеспечивать контроль эффективности принимаемых мер, а так же обеспечивать резервирование функций защиты на наиболее критичных участках.

12. Принцип простоты применения и апробированности защиты

СОБИ должна строиться на использовании простых элементарных защитных средств, для которых формально или неформально возможно доказать корректность исполнения защитных функций, проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование. Механизмы защиты, используемые СОБИ, должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных трудозатрат или малопонятных для пользователя действий (операций).

13. Принцип преемственности и совершенствования

СОБИ должна постоянно совершенствоваться на основе преемственности принятых ранее решений, анализа функционирования информационных систем и самой СОБИ с учётом лучшего опыта в области защиты информации.

14. Принцип персональной ответственности и минимизации привилегий

СОБИ должна предусматривать определение прав и ответственности каждого пользователя (в пределах полномочий) за обеспечение информационной безопасности. Распределение прав и ответственности должно в случае любого нарушения позволять определить круг виновных. Средства защиты, используемые в СОБИ, должны иметь возможность выделять пользователям и администраторам те права доступа, которые необходимы им для выполнения служебных обязанностей.

15. Принцип разделения обязанностей

СОБИ должна обеспечивать разделение прав и ответственности между сотрудниками налоговых органов, исключающее возможность нарушения критически важных для ФНС России процессов или создания бреши в защите одним пользователем.

16. Принцип разумной достаточности

При построении и использовании СОБИ необходимо соблюсти соответствие требуемого уровня затрат на обеспечение информационной безопасности, ценности информационных ресурсов и величины возможного ущерба субъектам, интересы которых затрагиваются в результате нарушения конфиденциальности, целостности и доступности информации. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать показатели работы информационных систем налоговых органов. Необходимо правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

Приложение № 7

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Функции, которые должны быть реализованы функциональными контурами исполнительного механизма СОБИ ФНС России

1. Контур поддержки доверенной среды

Контур поддержки доверенной среды (далее - контур ПДС) основывается на применении специальных программно-аппаратных средств. В состав подсистемы ПДС также входят средства защиты от вредоносных программ и вирусов (антивирусные средства). При построении контура ПДС необходимо учитывать, что входящие в него элементы должны реализовывать функции безопасности в объеме, необходимом для обеспечения требуемого уровня защищенности информационных систем налоговых органов.

Как правило (но, не ограничиваясь), элементы контура ПДС должны обеспечить:

неизменность применяемого в информационных системах налоговых органов общесистемного, прикладного и специального программного обеспечения;

проверку целостности программных средств защиты, а также общесистемного, прикладного и специального программного обеспечения информационных систем налоговых органов;

возможность проведения периодического тестирования функций безопасности информации, реализуемых СиЗИ;

возможность ведения, контроля и периодического обновления копий используемого в информационных системах налоговых органов общесистемного, прикладного и специального программного обеспечения;

предотвращение воздействия вредоносных программ на различные информационные узлы информационных систем налоговых органов и телекоммуникационной инфраструктуры ФНС России;

обнаружение атак на информационные системы налоговых органов со стороны внешних по отношению к ней сетей, в том числе глобальных информационных сетей (Internet);

контроль загрузки BIOS, операционной системы, компонент операционной системы, приложений, используемых в информационных системах налоговых органов;

регистрацию попыток несанкционированных действий с объектами защиты в информационных системах налоговых органов.

Входящие в состав ПДС средства защиты от вредоносных программ и вирусов (антивирусные средства) должны обеспечивать защиту отдельных рабочих станций (как стационарных, так и мобильных удаленных), серверов (веб-, почтовых, файловых хранилищ и различных серверов приложений) и всей информационной системы в целом. Средства защиты от вредоносных программ и вирусов (антивирусные средства) не должны значительно понижать производительность информационных систем налоговых органов и дополнительно обеспечивать:

обнаружение деструктивных воздействий на элементы информационных систем налоговых органов, в том числе обнаружение неизвестных кодов вирусов и вредоносных программ;

блокирование возможного распространения вирусов и уничтожение обнаруженных вредоносных программ;

восстановление информационных систем налоговых органов после возможных деструктивных воздействий;

централизованное автоматическое получение обновлений версий антивирусного программного обеспечения;

централизованное автоматическое получение обновлений баз данных вирусов от производителя и доведение их до субъектов;

управление и определение порядка антивирусной защиты рабочих станций (АРМ) пользователей и сетевых узлов информационных систем налоговых органов, управление процессом обновлений;

возможность удаленного управления и администрирования с рабочей станции (АРМ) администратора безопасности

ведение отчетов в удобной форме с возможностью настройки форм отчетов;

наличие действенных форм оповещения о происходящих событиях;

регистрации всех значимых для безопасности событий.

2. Контур идентификации и аутентификации субъектов

Контур идентификации и аутентификации субъектов (далее - контур ИАС) основывается на применении механизмов аутентификации, встроенных в средства защиты: средства защиты

информационных узлов от несанкционированного доступа к информации; средства усиленной (многофакторной) аутентификации.

При построении контура ИАС необходимо учитывать, что входящие в него элементы должны реализовывать функции безопасности, предусмотренные техническими требованиями Политики безопасности ФНС России или аналогичными требованиями* в объеме, необходимом для обеспечения требуемого уровня защищенности информационных систем налоговых органов. В состав контура ИАС входит удостоверяющий центр.

Как правило (но, не ограничиваясь), элементы контура ИАС должны обеспечить:

идентификацию и аутентификацию субъектов доступа до разрешения любых, связанных с обработкой защищаемых информационных ресурсов действий, персонификацию действий пользователей и администраторов информационных систем налоговых органов;

защиту пользователей информационных систем налоговых органов от раскрытия их идентификаторов и злоупотребления этим другими пользователями;

контроль присутствия пользователей в информационных системах налоговых органов, запрет работы пользователей после изъятия средства аутентификации из рабочих станций, серверов;

поддержку процесса идентификации (аутентификации) пользователей в случае использования субъектами доступа в качестве средств идентификации (аутентификации) цифровых сертификатов, а также средств подтверждения (проверки) подлинности электронных документов (электронной подписи) при исполнении функций и оказании государственных услуг.

Входящий в состав ИАС удостоверяющий центр должен дополнительно обеспечивать:

возможность хранения резервных копий программного обеспечения, необходимого для поддержания полного жизненного цикла цифровых ключей и цифровых сертификатов электронной подписи (генерация открытого и закрытого ключей ЭП, формирование цифрового сертификата ЭП, распределение ключей и сертификатов по протоколам CDP, LDAP данных аутентификации, отзыв сертификатов ЭП, проверка сертификатов ЭП, подтверждение сертификата ЭП);

размещение цифровых ключей и цифровых сертификатов ЭП на отчуждаемых носителях (USB ключи, Smart карты, ТМ токены) пользователей информационных систем налоговых органов, размещение списков цифровых сертификатов ЭП и списков отозванных сертификатов ЭП пользователей информационных систем налоговых органов на специальном сервере сертификатов;

взаимодействие при межведомственном информационном обмене и оказании государственных информационных услуг с внешними удостоверяющими центрами взаимодействующих органов государственной власти, кросс-сертификацию цифровых сертификатов, выданных удостоверяющими центрами взаимодействующих органов государственной власти, единую структуру сертификата ключа проверки электронной подписи;

ведение архива удостоверяющего центра, включающего документы, предоставляемые уполномоченным лицам при регистрации, изготовлении и выдаче, приостановлении, возобновлении действия и аннулировании сертификатов, получении информации о статусе сертификата ключа подписи, подтверждении подлинности электронной подписи в электронном документе, иную информацию, связанную с деятельностью удостоверяющего центра;

возможность восстановления работоспособности удостоверяющего центра после аварийных сбоев с минимальными информационными потерями и в короткие сроки.

Рабочая станция (АРМ) Удостоверяющего центра, предназначенная для формирования закрытых ключей и сертификатов пользователей информационных систем налоговых органов, должна размещается на автономной платформе, обеспечивать работу в автономном режиме и исключать возможность несанкционированного физического соединения с информационными системами налоговых органов. Формируемые цифровые сертификаты должны соответствовать формату, определенному рекомендациями и стандартами (RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile», RFC 4491 «Using the GOST R 34.10-94, GOST R.

3. Контур контроля и управления доступом субъектов

Контур контроля и управления доступом субъектов (далее - контур КДС) объединяет специализированные средства защиты от несанкционированного доступа к информации, встроенные (штатные) средства разграничения доступа общесистемного программного обеспечения и средств защиты информации (типовые настройки ОС, СУБД, телекоммуникационного оборудования). При построении контура КДС необходимо учитывать, что входящие в него элементы должны реализовывать функции безопасности, предусмотренные техническими требованиями Политики

безопасности ФНС России или аналогичными требованиями в объеме, необходимом для обеспечения требуемого уровня защищенности информационных систем налоговых органов.

Как правило (но, не ограничиваясь), элементы контура КДС должны обеспечить:

предоставление полномочий и разграничение прав доступа на основе данных идентификации и аутентификации пользователей, рабочих станций и серверов информационных систем, определение полномочий пользователей, разграничение доступа к прикладному программному обеспечению, информационным ресурсам и каналам связи телекоммуникационной инфраструктуры ФНС России;

определение единого набора правил (функций) защиты информации, реализуемых совокупностью средств защиты, контроля их выполнения и оперативного изменения;

формирование, исходя из единого набора правил защиты, индивидуальных правил (функций) защиты, реализуемых средствами защиты и телекоммуникационным оборудованием, исключение возможности их самостоятельного изменения пользователями;

запрет доступа в информационные системы налоговых органов не идентифицированных субъектов доступа, подлинность которых при аутентификации не подтвердилась;

доступность вычислительных возможностей информационных систем налоговых органов и/или потребных объемов памяти, предотвращение монополизации вычислительных возможностей каким-либо одним процессом (субъектом доступа).

4. Контур защиты потоков информации (ЗПИ)

Контур объединяет средства, реализующие криптографические преобразования данных (СКЗИ), средства подтверждения подлинности (целостности) информации (ЭП), средства создания виртуальных защищенных каналов (VPN-технологии). При построении контура ЗПИ необходимо учитывать, что входящие в него элементы должны реализовывать функции безопасности, предусмотренные техническим требованиями Политики информационной безопасности ФНС России или аналогичными требованиями** в объеме, необходимом для обеспечения требуемого уровня защищенности информационных систем налоговых органов.

Как правило (но, не ограничиваясь), элементы контура ЗПИ должны обеспечить:

организацию защищенных соединений (VPN каналов) между точками информационного взаимодействия налоговых органов и при осуществлении межведомственного взаимодействия;

защиту от несанкционированного доступа к информации, передаваемой по внешним открытым каналам при осуществлении межведомственного взаимодействия и оказании государственных услуг, а также по каналам внутри ФНС России;

управление потоками информации на основе меток конфиденциальности (мандатный принцип);

возможность реализации криптографических алгоритмов, рекомендованных уполномоченным федеральным органом исполнительной власти (определенных государственными стандартами) или разработанных (согласованных) уполномоченным федеральным органом исполнительной власти;

криптографическое преобразование защищаемой информации в процессе межведомственного информационного обмена, подтверждение подлинности передаваемой информации;

своевременную доставку пользователям информационных систем налоговых органов актуальной технологической информации (пароли, ключи, цифровые сертификаты электронной подписи), необходимой для исполнения функций и оказания (получения) государственных услуг;

формирование и поддержку полного жизненного цикла цифровых ключей и цифровых сертификатов (генерация, отзыв, распределение, проверка, подтверждение), используемых для аутентификации пользователей при исполнении государственных функций и оказании (получении) государственных услуг.

5. Контур регистрации и аудита событий

Контур регистрации и аудита событий (далее - контур РАС) основывается на применении встроенных в операционные системы и СУБД, прикладное и специальное программное обеспечение средств логирования действий и процессов, специализированных программных средств аудита и контроля за действиями пользователей информационных систем налоговых органов, средств регистрации, средств анализа защищенности и средства обнаружения и предупреждения атак (IDS/IPS). При

построении контура РАС необходимо учитывать, что входящие в него элементы должны реализовывать функции безопасности, предусмотренные техническими требованиями Политики информационной безопасности ФНС России в объеме, необходимом для обеспечения требуемого уровня защищенности информационных систем налоговых органов. Элементы контура должны обеспечить:

сбор и анализ данных об активности пользователей информационных систем налоговых органов, в том числе внешних, состоянии системного и прикладного программного обеспечения, всех действиях пользователей и администраторов информационных систем налоговых органов;

обнаружение атак на информационные системы налоговых органов со стороны внешних по отношению к ней сетей, в том числе глобальных информационных сетей (Internet);

оперативное оповещение подразделения ФНС России, отвечающего за обеспечение информационной безопасности о выявленных нарушениях правил (функций) защиты информации, потенциально опасных для безопасности информации действиях и ситуациях;

моделирование попыток несанкционированного доступа к ресурсам ФНС России, определение наиболее уязвимых мест в средствах защиты хранилищ информации (серверы), точках потенциального доступа извне к информации (межсетевые экраны), на рабочих станциях пользователей информационных систем налоговых органов;

анализ прав доступа к информационным ресурсам ФНС России пользователей, в том числе внешних по отношению к информационным системам налоговых органов;

выдачу отчета (оповещения) о найденных уязвимых местах и перечне мер, необходимых для их устранения;

регистрацию событий безопасности по параметрам для установленного класса защищенности и фильтрацию потока первичных событий с применением технических средств корреляции событий, оптимизирующих записи в журналах инцидентов информационной безопасности;

возможность резервного копирования и архивирования данных, образующихся в результате выполнения функций мониторинга, сбора и накопления информации о событиях безопасности и проведения операций над архивами;

возможность организации учёта отчуждаемых носителей, предназначенных для работы с защищаемыми информационными ресурсами.

Входящие в состав контура РАС средства анализа защищенности информационных систем налоговых органов должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационных систем налоговых органов.

Входящие в состав контура РАС системы обнаружения и предупреждения атак (IDS/IPS) должны иметь возможность регулярного обновления баз сигнатур и должны осуществлять выборочную контекстную проверку трафика в реальном масштабе времени, принимаемого от внешних пользователей информационных систем налоговых органов и взаимодействующих органов государственной власти.

6. Контур управления информационной безопасностью

При построении контура управления информационной безопасностью (далее - контур УИБ) необходимо учитывать, что входящие в него элементы должны реализовывать функции безопасности, предусмотренные техническим требованиями Политики информационной безопасности ФНС России в объеме, необходимом для обеспечения требуемого уровня защищенности информационных систем налоговых органов.

Как правило (но, не ограничиваясь), элементы контура УИБ должны обеспечить:

централизованное и децентрализованное (в случае нарушения функционирования каналов связи) управление элементами СиЗИ и отдельными подсистемами СОБИ;

администрирование безопасности информации информационных систем налоговых органов и телекоммуникационной инфраструктуры ФНС России;

контроль за безопасностью информации в информационных системах налоговых органов;

централизованное конфигурирование средств защиты информации и возможность изменения конфигурации СиЗИ при появлении новых рабочих мест пользователей, изменении телекоммуникационной инфраструктуры ФНС России, реконфигурации программного обеспечения;

передачу с применением технических средств (в гарантированно защищенном режиме) или при помощи защищенных носителей информации, индивидуальных правил (функций) защиты пользователю, их активизацию по запросу средства защиты информации либо уполномоченного лица;

возможность блокирования деятельности пользователей информационных систем налоговых органов, в том числе и внешних пользователей;

управление механизмами ликвидации нештатных (аварийных) ситуаций;

регистрацию всех значимых для безопасности событий для передачи в РАС;

доступ администратора безопасности к полным данным о работе каждого субъекта доступа.

_____

* Функциональные требования ГОСТ ИСО/МЭК 15408-2002 для класса FIA («Идентификация и аутентификация»), FPR («Приватность»)

** Функциональные требования ГОСТ ИСО/МЭК 15408-2002 для классов FCO («Связь»), FTP («Доверенный маршрут/канал»), FCS («Криптографическая поддержка»)

Приложение № 8

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Комплекс основных организационных, инженерно-технических и технических мер, реализуемых механизмом поддержки СОБИ ФНС России

1. Превентивные организационные меры

Превентивные меры должны найти отражение в организационно-распорядительных документах, определяющих положения о подразделениях налоговых органов, должностных регламентах (инструкциях) работников ФНС России и определять:

обязанности работников ФНС России о неразглашении и сохранении сведений ограниченного доступа (распространения);

порядок участия работников подразделений информационной безопасности налоговых органов в организации оценки соответствия оборудования и программного обеспечения требованиям информационной безопасности;

порядок участия работников подразделений информационной безопасности налоговых органов в организации аттестации объектов информатизации налоговых органов;

порядок проведения подразделениями центрального аппарата ФНС России и территориальных налоговых органов экспертизы проектов инженерных коммуникаций, размещения оборудования на предмет соответствия требованиям информационной безопасности, а также объем и содержание такой экспертизы;

состав подразделений налоговых органов, участвующих в категорировании объектов информатизации налоговых органов, а также порядок проведения такого категорирования;

порядок ведения учета ознакомления работников ФНС России с правилами работы с конфиденциальными информационными ресурсами ФНС России;

порядок участия администраторов информационных систем и администраторов информационной безопасности в проведении контроля и мониторинга состояния информационной безопасности;

порядок соблюдения мер информационной безопасности на рабочих местах работников ФНС России.

2. Ограничительные организационные меры

Ограничительные меры должны найти отражение в организационно-распорядительных документах, определяющих пропускной режим и порядок доступа на объекты и в помещения налоговых органов; состав объектов физической защиты, порядок их охраны; порядок учета, обеспечения сохранности и использования материальных средств и имущества; порядок транспортировки, доставки, разгрузки оборудования; внутренний распорядок. Ограничительные меры предполагают:

определение перечней критически важных объектов налоговых органов и объектов телекоммуникационной инфраструктуры ФНС России, защищаемых информационных ресурсов ФНС России, критически важных информационных систем ФНС России;

введение ограничений при доступе на объекты налоговых органов и в помещения, в которых размещаются критически важные технические средства обработки информации и элементы телекоммуникационной инфраструктуры ФНС России;

применение для идентификации и аутентификации работников ФНС России, посетителей и персонала обслуживающих организаций магнитных и электронных идентификаторов;

введением запрета неавторизованного доступа или доступа с паролем по умолчанию (принятым производителем оборудования или программного обеспечения) к управляющим портам, консольным портам, управляющим или административным аккаунтам любого коммуникационного оборудования и программного обеспечения;

введение ограничений на использование работниками ФНС России технических средств обработки информации на рабочих местах для обработки конфиденциальной информации, при присутствии сторонних работников, посетителей и персонала обслуживающих организаций;

введением запрета на использование в информационных системах налоговых органов оборудования и программного обеспечения в режимах, нарушающих условия лицензионного соглашения, определяемого изготовителем оборудования и программного обеспечения;

запрет на использование в информационных системах налоговых органов неучтенного оборудования и программного обеспечения;

введением запрета на использование фотографической, звукозаписывающей и видео аппаратуры в помещениях налоговых органов, за исключением санкционированных случаев.

3. Профилактические организационные меры

Профилактические меры должны найти отражение в организационно-распорядительных документах, определяющих планы и порядок повышения квалификации и переподготовки работников ФНС России; в положениях о подразделениях налоговых органов и должностных инструкциях руководителей подразделений ФНС России. Профилактические меры предполагают:

создание в ФНС России системы повышения уровня технической грамотности и информированности сотрудников ФНС России в области информационной безопасности, проведение инструктажей, семинаров, обучения сотрудников ФНС России;

организацию подготовки и переподготовки специалистов в области обеспечения информационной безопасности;

организацию контроля знаний работниками ФНС России основных положений Политики информационной безопасности ФНС России, должностных инструкций, в части обеспечения информационной безопасности и готовности работников налоговых органов к применению правил информационной безопасности;

организацию взаимодействия подразделений информационной безопасности налоговых органов с уполномоченными федеральными органами государственной власти (ФСТЭК России, ФСБ России) по вопросам правоприменения нормативных документов в области информационной безопасности и специальных средств защиты информации.

4. Стимулирующие организационные меры

Стимулирующие меры должны найти отражение в организационно-распорядительных документах, определяющих взаимоотношения между руководством и работниками ФНС России. Стимулирующие меры предполагают:

введение для работников ФНС России системы надбавок за работу с конфиденциальной информацией;

введение для работников ФНС России системы моральных поощрений, льгот и привилегий за работу без нарушений с конфиденциальной информацией.

5. Контрольные организационные меры

Контрольные меры должны найти отражение в организационно-распорядительных документах и:

определение состава подразделений, осуществляющих контроль физического доступа работников ФНС России и персонала обслуживающих организаций к техническим средствам обработки информации, на контролируемую территорию и в помещения налоговых органов, а также порядка такого контроля;

определение порядка организации уничтожения в подразделениях налоговых органов информационных отходов (бумажных, магнитных и т.д.) и утилизации технических средств обработки информации;

определение порядка и организация ведения в подразделениях налоговых органов учета материальных средств (технических средств обработки информации, отчуждаемых носителей информации, средств криптографической защиты информации), а также нематериальных активов (программного обеспечения);

определение порядка учета, хранения, эксплуатации и уничтожения в подразделениях налоговых органов ключей шифрования и электронных подписей;

определение порядка сервисного обслуживания технических средств обработки информации, информационных систем налоговых органов и оборудования телекоммуникационной инфраструктуры ФНС России, в том числе с привлечением сторонних организаций;

определение порядка осуществления контроля со стороны администраторов информационных систем налоговых органов за условиями эксплуатации средств обработки информации и объектов информатизации налоговых органов.

6. Дисциплинарные организационные меры

Дисциплинарные меры предполагают:

определение порядка разбора инцидентов информационной безопасности и проведения расследований по фактам нарушения правил обработки и защиты информации работниками налоговых органов;

определение порядка привлечения работников налоговых органов к ответственности за нарушение правил обработки и защиты информации.

7. Юридические организационные меры

Юридические меры должны найти отражение в контрактах и трудовых договорах с работниками ФНС России, в договорах (контрактах) с третьими лицами и предполагают:

заключение соглашений о неразглашении конфиденциальной информации с организациями, привлекаемыми для проектирования информационных систем, создания объектов информатизации налоговых органов, разработки прикладного программного обеспечения, сервисного обслуживания технических средств обработки информации и элементов телекоммуникационной инфраструктуры ФНС России, провайдерами телематических услуг;

включение в трудовые договоры (контракты) с работниками ФНС России положений о согласии субъекта на обработку своих персональных данных и обязательств о неразглашении персональных данных других субъектов, ставших известными в ходе исполнения служебных обязанностей;

включение в договоры с провайдерами телематических услуг, организаций, осуществляющих обработку информации по поручению ФНС России, положений о разделении полномочий в организации защиты информационных ресурсов ФНС России, наличию у провайдеров специально выделенных лиц, ответственных за информационную безопасность, круглосуточной службы реагирования на инциденты безопасности;

оформление и выдачу поручений организациям, осуществляющим обработку информации в интересах ФНС России, в которых определены: перечень действий (операций) с информацией, которые будут совершаться этой организацией; цели обработки; обязанности по соблюдению конфиденциальности и обеспечению безопасности информации при ее обработке; требования к защите обрабатываемой информации;

заключение с взаимодействующими организациями, с которыми осуществляется юридически значимый документооборот, Соглашений о взаимном признании электронных подписей;

приобретение для использования в информационных системах налоговых органов лицензионного программного обеспечения.

8. Обеспечивающие инженерно-технические меры

Обеспечивающие меры должны найти отражение в конструкторской и эксплуатационной документации, определяющей порядок размещения и эксплуатации систем жизнеобеспечения объекта, обеспечивающих устойчивую работу технических средств обработки информации или могущих повлиять на их работоспособность, в том числе эти документы должны содержать мероприятия и решения, направленные на обеспечение информационной безопасности при эксплуатации:

систем и средств электроснабжения критически важных объектов ФНС России;

систем и средств тепло- водоснабжения и канализации критически важных объектов ФНС России;

систем и средств вентиляции и кондиционирования критически важных объектов ФНС России;

зданий и сооружений критически важных объектов ФНС России в части пожароустойчивости;

зданий и сооружений критически важных объектов ФНС России в части сейсмоустойчивости.

9. Защитные инженерно-технические меры

Защитные меры должны найти отражение в конструкторской и эксплуатационной документации, определяющей порядок размещения и эксплуатации систем общей защиты объектов налоговых органов и систем общего обеспечения деятельности сотрудников ФНС России, в том числе эти документы должны содержать мероприятия и решения, направленные на обеспечение информационной безопасности при эксплуатации:

систем и средств противопожарной охраны объектов ФНС России;

средств грозозащиты объектов ФНС России;

систем и средств охранной сигнализации объектов ФНС России;

системы и средства телефонной связи ФНС России;

систем и средств оповещения сотрудников ФНС России;

экранированных помещений объектов ФНС России (при необходимости).

10. Комплекс технических мер

Комплекс технических мер объединяет меры, направленные на создание и поддержание в постоянной готовности резервных мощностей, позволяющих обеспечить при необходимости быстрое устранение нештатных ситуаций при эксплуатации информационных систем налоговых органов. Как правило (но, не ограничиваясь) технические меры должны предусматривать:

создание системы резервирования каналов связи телекоммуникационной инфраструктуры ФНС России;

создание резерва критического оборудования информационных систем налоговых органов;

создание системы резервного энергоснабжения критически важных объектов ФНС России.

Приложение № 9

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Состав

мероприятий, подлежащих реализации на исполнительском уровне СОБИ ФНС России

Все мероприятия, направленные на обеспечение ИБ ФНС России и реализуемые исполнительным механизмом и механизмом поддержки СОБИ ФНС России структурируются по слоям исполнительского уровня СОБИ. Выполнение данных мероприятий, в совокупности с применением специальных и встроенных в общесистемное ПО СЗИ, позволит обеспечить требуемый уровень защищенности ИР ФНС России.

1. Мероприятия, реализуемые СОБИ на физическом подуровне

Поставленные задачи защиты информации на физическом подуровне исполнительского уровня СОБИ достигаются:

выделением контролируемой зоны для объектов налоговых органов, в которой исключено бесконтрольное пребывание посторонних лиц и транспортных средств, обеспечением соблюдения пропускного режима и физической защиты объектов налоговых органов;

применением искусственных препятствий, затрудняющих проникновение на объекты налоговых органов (ворота, шлагбаумы, тамбуры и т.д.);

ознакомлением работников ФНС России с процедурой уведомления о различных нарушениях ИБ, вменением им в обязанности без промедления сообщать обо всех наблюдаемых или подозрительных случаях такого рода, установлением процедуры реагирования на нарушения информационной безопасности;

оборудованием объектов налоговых органов средствами противопожарной защиты, а особо ответственных помещений, предназначенных для хранения носителей защищаемых информационных ресурсов ФНС России - средствами пожаротушения, исключающими возможность физического уничтожения носителей в результате пожара;

обеспечением электрозащиты и грозозащиты объектов налоговых органов;

оборудованием помещений, где размещаются критичные элементы информационных систем налоговых органов многоконтурными техническими средствами охраны, а также созданием нескольких рубежей контроля входов в отдельные важнейшие помещения;

использованием для круглосуточного контроля электронных средств сигнализации, передающих на пульты службы охраны информацию о состоянии дверей, окон, стен, оград зданий, перемещении транспорта и людей по территории объектов налоговых органов;

ограничением доступа в конкретные помещения лиц, не имеющих специального разрешения, на основе применения устройств аутентификации (магнитные карты, коды, индукционные карточки и т.п.);

опечатыванием (пломбированием) уполномоченными лицами узлов и блоков информационных систем налоговых органов, участвующих в обработке защищаемых информационных ресурсов ФНС России, и к которым имеется доступ обслуживающего персонала при осуществлении ремонтных, наладочных и иных работ; осуществлением периодического контроля за опечатыванием данных устройств;

организацией учета технических средств обработки информации, носителей информации (в том числе дистрибутивов программного обеспечения), оборудованием помещений объектов налоговых органов специальными хранилищами для носителей информации, в том числе несгораемыми

сейфами, металлическими шкафами, созданием стабильных климатических условий для хранения носителей информации;

проверкой перед утилизацией элементов информационных систем налоговых органов всех компонент, включая носители информации (жесткие диски, дискеты, CD-диски и др.) на отсутствие защищаемой информации и лицензионного программного обеспечения;

страхованием технических средств обработки информации от физического разрушения технических средств и носителей информации от стихийных бедствий и форс-мажорных обстоятельств, недобросовестных действий работников налоговых органов, приводящих к полной или частичной утрате (уничтожению) защищаемых информационных ресурсов ФНС России;

организацией взаимодействия ФНС России с федеральными уполномоченными органами исполнительной власти по вопросам обеспечения защиты объектов налоговых органов, осуществлением контроля выполнения установленных требований по обеспечению режима защиты информационных ресурсов ФНС России.

2. Мероприятия, реализуемые СОБИ на технологическом подуровне

Поставленные задачи защиты информации на технологическом подуровне исполнительского уровня СОБИ достигаются:

использованием в информационных системах налоговых органов лицензионного программного обеспечения, принятием мер по соблюдению авторских прав на программное обеспечение, запретом исследования и копирования программного обеспечения;

созданием фонда алгоритмов и программ; проведением тестирования, учета и хранения копии всего программного обеспечения (разработанного или приобретенного), применяемого в информационных системах налоговых органов; запретом использования в информационных системах налоговых органов неучтенных копий программного обеспечения;

использованием в информационных системах налоговых органов общесистемного, специального и прикладного программного обеспечения (в том числе программного обеспечения средств защиты информации), потребительские и специальные функции которых подтверждены сертификационными испытаниями;

использованием в информационных системах налоговых органов общесистемного, прикладного и специального программного обеспечения (в том числе средств защиты информации), не содержащих технологических ошибок и недекларированных возможностей;

использованием специальных технологий программирования прикладного программного обеспечения, минимизирующих вероятность наличия дополнительных функциональных возможностей, используемых в дальнейшем для несанкционированного доступа к информации;

предупреждением внесения несанкционированных изменений в прикладное программное обеспечение в процессе разработки и эксплуатации; периодической сверкой программного обеспечения с эталонными копиями, хранимыми отдельно в фонде алгоритмов и программ;

применением специальных сертифицированных антивирусных средств тестирования и восстановления программного обеспечения, программ контроля и обеспечения целостности и неизменности программного обеспечения при его загрузке и использовании, алгоритмов самотестирования и самовосстановления исполняемого кода программного обеспечения;

применением в информационных системах налоговых органов и телекоммуникационной инфраструктуре ФНС России защищенных средств обработки информации, исключающих возможность несанкционированного съема информации за счет побочных электромагнитных излучений и наводок (имеющих сертификат соответствия требованиям электромагнитной совместимости или документ, подтверждающий соответствие технических средств отечественным стандартам по ЭМС - по классу не ниже Б по ГОСТ Р 51318.22-99);

выполнением на объектах налоговых органов установленных требований по размещению технических средств обработки информации, организации их бесперебойного и гарантированного электропитания, заземления;

размещением технических средств обработки информации (средств отображения и изготовления документов) в местах, исключающих возможность визуального просмотра выводимой на них информации лицами, не имеющими к ней доступа;

резервированием технических средств обработки информации информационных систем налоговых органов, используемых на наиболее ответственных участках информационных систем налоговых органов или для обработки оперативной информации;

применением защищенных (в том числе сертифицированных) вспомогательных технических средств и систем, не создающих технических каналов утечки защищаемой информации;

обеспечением надежного сервисного обслуживания технических средств обработки информации информационных систем налоговых органов с привлечением (по необходимости) организаций, имеющих соответствующие лицензии.

3. Мероприятия, реализуемые СОБИ на пользовательском подуровне

Поставленные задачи защиты информации на пользовательском подуровне исполнительского уровня СОБИ достигаются:

созданием в налоговых органах разрешительной системы допуска сотрудников ФНС России к обработке защищаемой информации, установлением персональной ответственности сотрудников ФНС России за нарушения установленного порядка применения информационных технологий при обработке информации, правил хранения и передачи защищаемой информации, организацией инструктажа сотрудников ФНС России;

присвоением пользователям идентификационных меток (идентификаторов) и применением средств идентификации; проверкой принадлежности идентификаторов к пользователю и подтверждению его подлинности (аутентификация); ограничения прав пользователей информационных систем налоговых органов по доступу к средствам обработки информации;

разграничением полномочий пользователей информационных систем налоговых органов по доступу к защищаемым информационным ресурсам ФНС России и сервисам, использованием средств адресации по полномочиям, проверкой полномочий с помощью программно-аппаратных средств защиты информации;

изоляцией пользователей информационных систем налоговых органов от возможности управления и изменения параметров программно-аппаратных средств защиты информации, в том числе средств криптографической защиты информации;

организацией управления потоками информации между пользователями информационных систем налоговых органов, исключением возможности несанкционированного перенаправления потоков информации и изменения правил доступа к информационным ресурсам ФНС России и сервисам;

регистрацией попыток несанкционированного обращения к информационным ресурсам ФНС России, сервисам информационных систем налоговых органов и последующим анализом попыток и аномальной активности пользователей по обращению к информационным ресурсам ФНС России;

применением специальных средств блокировки клавиатуры, диска или каталога без выключения технических средств обработки информации в случае временного оставления рабочего места пользователем;

уничтожением фрагментов данных в оперативном запоминающем устройстве, регистрах процессора и запоминающего устройства принтера по окончании работы с данными, применением защиты данных на файловом уровне, на жестком диске, съемных носителях;

локализацией в отдельном автономном сегменте технологических рабочих станций, предназначенных для разработки и отладки прикладного программного обеспечения;

разнесением возможности использования (запуска) программных средств разработки и рабочих программ (запретом совместного хранения компиляторов, редакторов и других системных утилит с рабочими системами), использованием разных процедур входа в рабочие и тестируемые системы.

4. Мероприятия, реализуемые СОБИ на сетевом (локальном) подуровне

Поставленные задачи защиты информации на сетевом (локальном) подуровне исполнительского уровня СОБИ достигаются:

созданием защищенной оболочки (периметра) вокруг информационных систем налоговых органов в целом, и отдельных их сегментов с применением средств защиты информации от несанкционированных действий со стороны пользователей открытых сетей общего пользования, в том числе глобальной информационной сети Интернет;

созданием сегментов обработки и хранения информационных ресурсов ФНС России, объединенных функциональной необходимостью, степенью конфиденциальности информации и местоположением рабочих станций пользователей, специальных технологических сегментов, выделением в обособленный сегмент средств и Инфраструктурных ИР, обеспечением взаимной устойчивости защиты одних сегментов к компрометации средств защиты других сегментов;

созданием зон повышенной безопасности для информационных ресурсов ФНС России, имеющих более высокий уровень защищенности;

разграничением полномочий групп пользователей информационных систем налоговых органов (в том числе внешних) по доступу к информационным ресурсам ФНС России по степени конфиденциальности и по функциональной необходимости обращения к защищаемым информационным ресурсам;

исключением возможности несанкционированного перенаправления потоков информации и изменения правил доступа к информационным ресурсам ФНС России;

исключение возможности несанкционированного перенаправления потоков информации, циркулирующих во вспомогательных средствах и системах (информация системы охраны, видеонаблюдения, телефонии, управления и пр.) и изменения правил доступа к ним;

регистрацией аномальной активности пользователей информационных систем налоговых органов при обращении к информационным ресурсам ФНС России;

реализацией заданной дисциплины взаимодействия (аутентификация и/или защита канала) для каждого защищенного соединения, доступом в заданном защищенном режиме только для зарегистрированных (в том числе и для мобильных и внешних) пользователей информационных систем налоговых органов;

резервированием основных хранилищ информационных ресурсов ФНС России и Инфраструктурных ИР вспомогательных средств и систем (системы охраны, видеонаблюдения, управления, диспетчерской связи), использованием средств архивации данных;

организацией буферного сегмента для размещения общедоступных информационных ресурсов ФНС России.

5. Мероприятия, реализуемые СОБИ на канальном подуровне

Поставленные задачи защиты информации на канальном подуровне исполнительского уровня СОБИ достигаются:

созданием защищенного от несанкционированных действий виртуального канала для обращения удаленных (мобильных) пользователей (сегментов) информационных систем налоговых органов к информационным ресурсам ФНС России через внешние телекоммуникационные сети, в том числе глобальную информационную сеть Интернет, контролем списка партнеров по защищенному/незащищенному взаимодействию независимо на каждом физическом интерфейсе;

применением специальных выделенных каналов обмена информацией для связи с удаленными пользователями (сегментами) информационных систем налоговых органов;

реализацией заданной дисциплины взаимодействия (аутентификация и/или защита канала) для каждого защищенного соединения, доступом в заданном защищенном режиме только зарегистрированных (в том числе и мобильных и внешних) пользователей информационных систем налоговых органов;

созданием системы администрирования безопасности информационных систем налоговых органов и управления информационной безопасностью ФНС России с рабочих станций администраторов безопасности информационных систем налоговых органов;

поддержкой защищенных сетевых соединений только с зарегистрированными пользователями информационных систем налоговых органов (в том числе внешних) и с установленными параметрами (атрибутами) защиты соединения для каждого конкретного пользователя;

применением средств криптографической защиты информации, регулированием стойкости защиты путем одновременного применения криптографических библиотек разных производителей, созданием инфраструктуры управления открытыми ключами пользователей информационных систем налоговых органов.

Приложение № 10

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Состав

средств защиты информации и требования по их размещению на элементах информационных систем налоговых органов

1. Требования к СиЗИ, обеспечивающим физический подуровень защиты СОБИ

Технические средства охраны, видеонаблюдения, разграничения доступа, входящие в состав СиЗИ на физическом подуровне должны, как минимум, обеспечивать выделение особых зон внутри объектов ФНС России для размещения критически важных технических средств обработки информации информационных систем налоговых органов, имеющих особый режим допуска, контроль за пожарной безопасностью и контроль за отсутствием посторонних лиц в пределах контролируемой зоны объектов информатизации. С этой целью должны использоваться следующие средства защиты:

специальные технические средства идентификации и аутентификации сотрудников ФНС России, посетителей, работников сервисных организаций - на входах в выделенные особые зоны внутри объектов налоговых органов, имеющих особый режим допуска (серверные комнаты, машинные залы ЦОД, хранилища информационных ресурсов ФНС России, помещения для размещения коммутационного оборудования телекоммуникационной инфраструктуры ФНС России, помещения для ведения конфиденциальных переговоров);

системы охранной и пожарной сигнализации с оповещением на центральный пост охраны - помещения налоговых органов, в которых размещены элементы информационных систем налоговых органов;

средства видеонаблюдения и документирования изображений - периметр охраняемой территории объектов налоговых органов, помещения охранных структур.

2. Требования к СиЗИ, обеспечивающим технологический подуровень защиты СОБИ

Встроенные функции защиты общесистемного программного обеспечения (ОС, СУБД), и специальные технические СЗИ, используемые в информационных системах налоговых органов и входящие в состав СиЗИ на технологическом подуровне должны, как минимум, обеспечивать:

контролируемый допуск зарегистрированных пользователей к работе в информационных системах налоговых органов;

создание защитного периметра вокруг элементов информационных систем налоговых органов;

создание индивидуальной среды деятельности каждого зарегистрированного пользователя информационных систем налоговых органов;

запрет доступа пользователей информационных систем налоговых органов к неиспользуемым сервисам общесистемного программного обеспечения (ОС, СУБД);

ограничение использования пользователями информационных систем налоговых органов сервисов операционных систем, осуществляющих мониторинг сети;

исключение несанкционированной загрузки пользователями информационных систем налоговых органов операционных систем с внешних дисководов (FDD, CD и др.);

исключение несанкционированного использования пользователями информационных систем налоговых органов внешних накопителей;

блокирование гостевых входов (учетных записей типа «guest») на серверах всех типов;

блокирование доступа извне к неиспользуемым портам информационных систем налоговых органов;

ограничение числа пользователей информационных систем налоговых органов с правом локальной регистрации;

ограничение числа пользователей информационных систем налоговых органов с правом доступа к системному реестру;

изоляцию пользователей информационных систем налоговых органов от возможности управления и изменения параметров средств защиты информации.

3. Требования к СиЗИ, обеспечивающим пользовательский подуровень защиты СОБИ

СиЗИ на пользовательском подуровне должна предусматривать оборудование технических средств обработки информации информационных систем налоговых органов (как минимум) следующими средствами защиты информации:

программно-аппаратными средствами обеспечения доверенной загрузки (как правило, входят в состав средств защиты от несанкционированного доступа к информации) - все технические средства обработки информации информационных систем налоговых органов, использующие общесистемное программное обеспечение;

средствами авторизации и разграничения полномочий пользователей (средства защиты от несанкционированного доступа к информации) - рабочие станции (АРМ) внутренних пользователей информационных систем налоговых органов, имеющих доступ к защищаемым информационным ресурсам ФНС России и участвующих в процессе их обработки, АРМ администраторов информационных систем, администраторов информационной безопасности, технологические АРМ программистов и обслуживающего персонала информационных систем налоговых органов;

средствами блокирования процессов обработки защищаемой информации и изменений правил доступа к информационным ресурсам ФНС России пользователями информационных систем налоговых органов, не имеющими соответствующих прав (серверы и устройства хранения информационных ресурсов ФНС России);

средствами управления потоками информации между пользователями информационных систем налоговых органов, исключающими возможность несанкционированного перенаправления потоков информации и изменения правил доступа к информационным ресурсам ФНС России (все АРМ

пользователей информационных систем налоговых органов, серверы и устройства хранения информационных ресурсов ФНС России);

средствами регистрации неправомерных действий с информацией и системных событий (как правило, осуществляется средствами защиты от несанкционированного доступа к информации, средствами логирования операционных систем и систем управления базами данных (АРМ администраторов информационной безопасности, серверы и устройства хранения информационных ресурсов в информационных системах налоговых органов);

средствами защиты от вредоносных программ - все серверы, АРМ и устройства хранения информационных ресурсов, участвующие в процессе обработки защищаемых информационных ресурсов ФНС России.

4. Требования к СиЗИ, обеспечивающие сетевой (локальный) подуровень защиты СОБИ

Реализация требований настоящего раздела направлена на создание защитной оболочки по периметру информационных систем налоговых органов и их отдельных сегментов, обеспечивающей исключение возможности утечки информации ограниченного доступа в другие сегменты, скрытие топологии сегмента (адресная информация) и служебной информации о нём (имена пользователей, пароли), предотвращающей несанкционированное проникновение пользователей информационных систем налоговых органов в пределы сегмента, а также обеспечивающей санкционированный обмен информацией между сегментами информационных систем налоговых органов и межведомственный информационный обмен. СиЗИ на сетевом (локальном) подуровне должна предусматривать оборудование элементов информационных систем налоговых органов (как минимум) следующими средствами защиты информации:

межсетевыми экранами - элементы информационных систем налоговых органов, расположенные в точках входа/выхода в информационные системы налоговых органов и их обособленные сегменты (серверы, маршрутизаторы, коммутаторы, шлюзы, мосты), удаленные и мобильные рабочие станции (АРМ) пользователей информационных систем налоговых органов;

средствами защиты от несанкционированного доступа из внешних сетей и организации защищенных соединений с удаленными и мобильными АРМ пользователей информационных систем налоговых органов (могут входить в состав межсетевых экранов) - все АРМ пользователей информационных систем налоговых органов, в том числе удаленные и мобильные, все серверы, устройства хранения и отображения защищаемой информации;

средствами повышенной аутентификации пользователей и защиты от несанкционированного доступа к информации (как правило, осуществляется средствами межсетевых экранов) - удаленные и мобильные АРМ пользователей информационных систем налоговых органов, предназначенные для обработки защищаемых информационных ресурсов ФНС России;

средствами защиты от вредоносных программ, обеспечивающие предварительную фильтрацию известных вирусов, вредоносных программ, а также любого подозрительного кода (сканирующие программы фильтрации проходящего трафика FTP, HTTP, SMTP и т.д.), и блокирование трафика в случае обнаружения кода вредоносной программы - элементы информационных систем налоговых органов, расположенные в точках входа/выхода в информационные системы налоговых органов (шлюзы сопряжения, серверы);

специальными программными фильтрами, обеспечивающими возможность перекодировки содержимого электронной корреспонденции (различающие вложенные файлы формата MIME, UUENCODE и архивные файлы), антивирусными средствами, а также применением встроенных в общесистемное ПО функции защиты от записи в каталоги, в которых хранятся программные файлы - элементы информационных систем налоговых органов, расположенные в точках размещения файловых, почтовых серверов информационных систем налоговых органов;

средствами обнаружения и регистрации неправомерных действий с информацией и внешних атак на периметр сегмента - элементы информационных систем налоговых органов, расположенные в точках входа/выхода в информационные системы налоговых органов и их обособленные сегменты (серверы, маршрутизаторы, коммутаторы, шлюзы, мосты), АРМ администраторов информационной безопасности;

средствами аудита, обнаружения и предупреждения о вторжениях (атаках) - элементы информационных систем налоговых органов, расположенные в точках входа/выхода в информационные системы налоговых органов (серверы, маршрутизаторы, коммутаторы, шлюзы, мосты).

5. Требования к СиЗИ, обеспечивающие канальный уровень защиты СОБИ

Реализация требований настоящего раздела направлена на обеспечение защиты информационных ресурсов ФНС России при передаче данных по каналам связи при информационном взаимодействии отдельных сегментов и/или пользователей информационных систем налоговых органов, а также при межведомственном информационном обмене. Количество точек входа/выхода в информационные системы налоговых органов, через которые осуществляется межведомственный информационный

обмен, а также взаимодействие с внешними пользователями информационных систем налоговых органов, должно быть ограниченным и минимально необходимым. Адресное пространство информационных систем налоговых органов должно быть самостоятельным и не может являться подмножеством адресного пространства информационно-телекоммуникационных сетей общего пользования. СиЗИ на канальном подуровне должна предусматривать оборудование элементов информационных систем налоговых органов, как минимум, следующими средствами защиты информации:

средствами защиты от несанкционированного доступа из внешних сетей к существующим соединениям и организации защищенных соединений информационных систем налоговых органов с информационными системами других органов государственной власти на основе применения программных или программно-аппаратных средств, использующих технологии межсетевых экранов и средств создания защищенного от несанкционированных действий виртуального канала связи (VPN-технологий) (могут входить в состав средств защиты предыдущего подуровня) - все АРМ пользователей, все серверы и устройства хранения и отображения защищаемой информации информационных систем налоговых органов;

специальными средствами формирования и поддержания доверенных каналов обмена информацией между обособленными сегментами информационных систем налоговых органов и информационными системами других органов государственной власти с которыми осуществляется межведомственное взаимодействие (средства формирования виртуальных защищенных каналов - VPN-технологии) (точки входа/выхода в информационную систему органа государственной власти (серверы, маршрутизаторы, коммутаторы);

средствами регистрации неправомерных действий с информацией и внешних атак на периметр информационной системы органа государственной власти - элементы информационных систем налоговых органов, расположенные в точках входа/выхода в информационные системы налоговых органов и их обособленные сегменты (серверы, маршрутизаторы, коммутаторы, шлюзы, мосты), АРМ администраторов информационной безопасности;

средствами криптографической защиты информации (могут реализовываться средствами VPN-технологий) и средствами распределения сертификатов ключей по открытым сетям - все АРМ, подключаемые к информационным системам налоговых органов не через выделенные каналы связи, все средства обмена информацией с территориально разнесенными сегментами информационных систем налоговых органов;

специальными программными средствами обнаружения вторжений в информационные системы налоговых органов, аудита информационной безопасности информационных систем налоговых органов и выявления уязвимых мест в средствах защиты веб-серверов, межсетевых экранов, серверов и АРМ - АРМ администраторов информационной безопасности информационных систем налоговых органов;

специальными программными и программно-аппаратными средствами, обеспечивающими скрытие адресного пространства (топологии) информационных систем налоговых органов (NAT-технологии) - элементы информационных систем налоговых органов, расположенные в точках входа/выхода в информационные системы налоговых органов и их обособленные сегменты (серверы, маршрутизаторы, коммутаторы, шлюзы, мосты).

Дополнительно к специальным функциям защиты информации, определенных с установленным классом защищенности для межсетевых экранов, средства создания защищенного от несанкционированных действий виртуального канала связи (применение VPN-технологий) должны обеспечивать:

идентификацию и аутентификацию пользователей информационных систем налоговых органов, получающих доступ к защищенным от несанкционированных действий виртуальным каналам по идентификатору;

поддержку внешних устройств усиленной аутентификации пользователей информационных систем налоговых органов, контроль их присутствия в информационной системе и отключение пользователей после извлечения ими средства аутентификации;

аутентификацию пользователей информационных систем налоговых органов и средств создания защищенных виртуальных каналов удаленных сегментов с заранее неизвестным сетевым адресом;

аутентификацию входящих/исходящих сообщений (пакетов) отдельных пользователей информационных систем налоговых органов;

запрет доступа не идентифицированного субъекта (в том числе пользователя), подлинность идентификации которого при аутентификации не подтвердилась;

скрытие топологии информационной системы органа государственной власти с использованием туннелирования и векторизации входящих/исходящих сообщений (пакетов);

контроль входящих/исходящих сообщений (пакетов) и регистрацию попыток несанкционированных обращений и действий в информационной системе органа государственной власти;

расширенную фильтрацию входящих/исходящих пакетов на основе сетевых адресов;

регистрацию и учёт фильтруемых пакетов;

возможность подключения внешних сертифицированных криптографических модулей;

одновременную поддержку открытых и закрытых соединений;

централизованное управление конфигурированием и настройку средств создания защищенных от несанкционированных действий виртуальных каналов для удаленных сегментов информационных систем налоговых органов;

формирование и хранение ключей пользователей всех сегментов информационных систем налоговых органов на автономном защищенном носителе.

При передаче защищаемой информации по открытым каналам связи должны обеспечиваться:

применение средств криптографической защиты информации соответствующего уровня защищенности;

возможность формирования и распределения криптографических ключей, паролей пользователей информационных систем налоговых органов;

контроль и регистрация изменений режимов работы технических средств обработки информации, нарушений безопасности

персонификация действий пользователей информационных систем налоговых органов;

выдача инструкций пользователям при нештатных (аварийных) ситуациях;

управление механизмами ликвидации нештатных (аварийных) ситуаций.

Приложение № 11

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

Типы сегментов информационных систем налоговых органов

Сегментирование информационных систем налоговых органов может проводиться либо по функциональному признаку, то есть по степени необходимости той или иной группе пользователей обращаться к определенным информационным ресурсам, либо по признаку ограничения доступа, то есть по степени конфиденциальности информации.

Деятельность ФНС России связана с необходимостью одновременной обработки информации разной степени конфиденциальности в пределах одного функционального признака (функциональной задачи, государственной информационной услуги), поэтому сегменты информационных систем налоговых органов, формируемых по функциональному признаку, могут и должны включать в себя разные по степени разграничения доступа сегменты информационных систем. Взаимодействие этих сегментов не должно снижать установленного уровня безопасности для информационных ресурсов ФНС России.

Границей сегментов информационных систем налоговых органов является внешний по отношению к сегменту порт коммутирующих (маршрутизирующих) устройств или средства защиты информации, установленных в точке сопряжения с другими сегментами.

Выделяются следующие типы сегментов информационных систем налоговых органов:

1) Закрытые сегменты, предназначены для обработки информационных ресурсов ФНС России, содержащих конфиденциальную информацию (Конфиденциальные налоговые ИР, ИР персональных данных, частично Служебные ИР, Технологические ИР). Данные сегменты объединяют рабочие станции (АРМ) пользователей информационных систем налоговых органов, имеющих доступ к такой информации, средства отображения, хранения, обработки, ввода, вывода, коммутации и маршрутизации такой информации, а также собственно конфиденциальные ИР. Закрытых сегментов может быть несколько, исходя из степени ограничения доступа к информации. Закрытые сегменты формируют:

внутриведомственные контуры взаимодействия налоговых органов, доступные только сотрудникам ФНС России в пределах одного отдельного (самостоятельного) объекта налоговых органов;

ведомственный контур взаимодействия налоговых органов, доступный всем сотрудникам ФНС России независимо от объектовой принадлежности;

межведомственный контур взаимодействия, предназначенный для межведомственного обмена конфиденциальной информацией с другими федеральными органами власти.

2) Открытые сегменты, предназначены для обработки открытых, но не общедоступных информационных ресурсов ФНС России (Служебные ИР, Коммерческие ИР, Открытые налоговые ИР, Открытые регистрационные ИР, частично Служебные ИР, Инфраструктурные ИР). Данные сегменты объединяют рабочие станции (АРМ) пользователей информационных систем налоговых органов, не имеющих полного доступа к информационным ресурсам ФНС России ограниченного доступа, средства отображения, хранения, обработки, ввода, вывода, коммутации и маршрутизации такой информации, а также информационные ресурсы ФНС России содержащие такую информацию. Открытые сегменты входят в состав:

межведомственного контура взаимодействия, предназначенного для межведомственного обмена открытой, но не общедоступной информацией с другими федеральными органами власти;

внешнего контура взаимодействия с зарегистрированными и прошедшими верификацию внешними пользователями информационных систем налоговых органов (налогоплательщики), которые наделены определенными правами доступа к информационным ресурсам ФНС России.

3) Буферные сегменты, предназначены для обработки открытых общедоступных информационных ресурсов ФНС России (Общедоступные ИР). Данные сегменты объединяют средства обработки и хранения информации, предназначенной для внешних пользователей (открытые порталы, открытые почтовые и публичные серверы и пр.), а также средства обеспечения доступа к такой информации самих внешних пользователей. Буферные сегменты формируют:

открытый контур взаимодействия, предназначенный для обмена информацией в внешними пользователями информационных систем налоговых органов, не имеющих регистрацию и не входящих в состав информационных систем налоговых органов.

Открытые общедоступные информационные ресурсы ФНС России, хранящиеся в буферном сегменте должны иметь актуализируемый дубликат на средствах хранения информации открытого сегмента.

4) Удаленные сегменты (открытые или закрытые), объединяют рабочие станции (АРМ) удаленных (или мобильных) пользователей информационных систем налоговых органов, средства отображения, хранения, ввода, вывода, передачи информации.

Приложение № 12

к Концепции информационной безопасности

Федеральной налоговой службы,

утв. приказом Федеральной

налоговой службы

от 13 января 2012 г. № ММВ-7-4/6@

(справочное)

Нормативно-методические документы и Стандарты по обеспечению безопасности информации

Приказ Директора ФСБ России от 09.02.2005 № 66, (зарегистрирован в Минюсте России 03.03.2005, № 6382) «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Приказ Директора ФСТЭК России от 05.02.2010 № 58 (зарегистрирован в Минюсте России 19.02.2010, № 16456) «Положение о методах и способах защиты информации в информационных системах персональных данных».

Приказ Директора ФСТЭК России № 74 от 14.03.2009 «Положение о Реестре ключевых систем информационной инфраструктуры»

Совместный приказ ФСТЭК России, ФСБ России и Минкомсвязи России от 13.02.2008 № 55/86/20 (зарегистрирован в Минюсте России 03.04.2008, регистрационный № 11462.) «Порядок проведения классификации информационных систем персональных данных».

РД. ФСТЭК России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации», Москва, 1998 г.

РД. ФСТЭК России «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации», Москва, 1998 г.

РД. ФСТЭК России. «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР)», Москва, 1997 г. (с изменениями от 2005, 2006, 2008 годов).

РД. ФСТЭК России. «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», Москва, 2002 г.

РД. ФСТЭК России. «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры», 2007 г.

РД. ФСТЭК России. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», 2007 г.

«Временные требования к устройствам типа межсетевые экраны», ФСБ России, 2004 г.

«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», ФСТЭК России 2007 г.

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», ФСБ России, 2008 г.

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008 г.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008 г.

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», письмо ФСБ России, 2008 г., № 149/54-144.

ГОСТ Р 50922-1996 «Защита информации. Основные термины и определения».

ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

ГОСТ ИСО/МЭК 15408-2-2002 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью».

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, влияющие на информацию. Общие положения».

ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

Р 50.1.053-2005. «Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации».

Р 50.1.056-2005 «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения».

ISO/IEC 17799 «Информационные технологии. Технологии безопасности. Практика управления информационной безопасностью».

ISO/IEC FDIS 27001 «Информационные технологии. Технологии безопасности. Система управления информационной безопасностью. Требования».

Приказ Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@ “Об утверждении Концепции информационной безопасности Федеральной налоговой службы”

Текст приказа официально опубликован не был