Содержание

Введение

Согласно Доктрине информационной безопасности Российской Федерации, утверждѐнной приказом Президента Российской Федерации № 1895 от 09 сентября 2000 г., Россия в значительной степени отстаѐт от ведущих стран в сфере информатизации органов исполнительной власти, к каковым относится Федеральное казначейство. Несмотря на разницу почти в 15 лет, данный тезис до сих пор остаѐтся крайне актуальным, можно сказать злободневным.

Федеральное казначейство (Казначейство России) является федеральным органом исполнительной власти, осуществляющим в соответствии с законодательством Российской Федерации правоприменительные функции по обеспечению исполнения федерального бюджета, кассовому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, предварительному и текущему контролю ведения операций со средствами федерального бюджета главными распорядителями, распорядителями и получателями средств федерального бюджета [23].

В условиях существующего административно-территориального деления страны органы Федерального казначейства (ФК) представляют собой многоуровневую и территориально распределѐнную систему, реализованную на трѐх уровнях: Центральный аппарат ФК (ЦАФК), территориальные управления ФК по субъектам Российской Федерации (УФК) и подчинѐнные им Отделения УФК (ОФК) в городах и районах этих городов. Органы ФК в рамках осуществления своих полномочий в установленной сфере деятельности взаимодействуют с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, Центральным банком Российской Федерации, общественными объединениями и иными организациями.

В органах ФК, будь то ЦАФК, УФК или ОФК, обрабатываются внушительные объѐмы информации с ограниченным доступом. Это и различного рода

персональные данные, и государственная тайна. Указанная информация периодически подвергается угрозам безопасности информации. Однако в данной работе защита информации, составляющей государственную тайну, не рассматривается в силу объективных причин.

Основными особенностями информационной и телекоммуникационной инфраструктуры органов ФК являются:

- территориальная распределѐнность;

- объединение в единую систему большого количества разнотипных технических средств обработки, хранения и передачи информации;

- разнообразие решаемых задач, категорий и типов обрабатываемых сведений (данных), технологически сложные режимы автоматизированной обработки информации;

- непосредственный доступ к вычислительным и информационным ресурсам большого числа различных категорий пользователей (источников и потребителей информации) и технического персонала, обслуживающего средства вычислительной техники;

- наличие разнообразных каналов связи со сторонними организациями;

- непрерывность функционирования, высокая интенсивность информационных потоков;

- наличие функциональных подсистем с различными требованиями по уровням защищѐнности.

Объекты информатизации органов ФК включают:

- технологическое оборудование (средства вычислительной техники, сетевое и кабельное оборудование);

- информационные ресурсы, содержащие сведения ограниченного доступа, общедоступную информацию, критически важную технологическую и управляющую информацию, иные сведения, представленные в виде документов или записей на носителях на магнитной, оптической и другой основе, информационных физических полях, массивах и базах данных;

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

- телекоммуникационные системы связи и передачи данных (средства телекоммуникации);

- режимные и служебные помещения, в которых циркулирует информация ограниченного доступа, общедоступная информация;

- технические средства и системы, не обрабатывающие защищаемую информацию (вспомогательные технические средства и системы), но размещѐнные в помещениях, где она обрабатывается (циркулирует).

В общем виде информационная и телекоммуникационная инфраструктура органов ФК представляется совокупностью автоматизированных систем на базе локальных вычислительных систем центрального аппарата ФК и территориальных органов Федерального казначейства, объединѐнных Ведомственной транспортной (телекоммуникационной) сетью (ВТС). Защита информации в каналах связи ВТС осуществляется с использованием средств криптографической защиты информации (СКЗИ).

Локальные вычислительные сети, предназначенные для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, образуют объектовые конфиденциальные контуры и, как правило, связаны между собой посредством Ведомственной транспортной сети.

Для взаимодействия с сетями связи общего пользования и доступа в сеть Интернет на объектах органов ФК создаѐтся специализированная ЛВС (Интернет-контур), не имеющая сетевых соединений с конфиденциальным и закрытым контурами.

Автоматизированные системы органов ФК условно можно разделить на следующие классы:

- существующие автоматизированные системы, в составе которых используется специально разработанное прикладное программное обеспечение (ППО) и системы управления базами данных (СУБД);

- предполагаемые к внедрению перспективные автоматизированные системы, в составе которых также используется специализированное ППО и СУБД;

- существующие автоматизированные системы, функциональность которых основана на использовании стандартных возможностей клиентских и серверных операционных системах семейства MSWindows, офисных и почтовых приложений для этих ОС, браузеров доступа к ресурсам сети Интернет, портальных решений, других общесистемных утилит.

Основное назначение прикладных систем – автоматизация возложенных на органы ФК функций реализации бюджетного процесса и обеспечение административно-хозяйственной, финансовой, кадровой, и других сфер деятельности органов ФК. Сюда же входят различные системы электронного документооборота, аналитические системы, системы мониторинга и управления эксплуатацией.

Системы общего назначения имеют справочно-информационный характер и базируются, как правило, на предоставлении или использовании различных сервисов сетей связи общего пользования и, в первую очередь, сети Интернет.

Функции безопасности в каждой из этих автоматизированных систем реализуются (должны реализовываться) одним из следующих способов:

- для автоматизированных систем общего назначения используются функции безопасности на уровне ОС средств вычислительной техники. В качестве средств защиты информации вычислительных узлов применяются штатные возможности клиентских и серверных ОС семейства MSWindows, а также готовые и доступные на рынке антивирусные средства защиты. Защита от сетевых компьютерных атак в этих системах при взаимодействии с сетями связи общего доступа основывается на применении межсетевых экранов и создании демилитаризованных зон;

- для прикладных АС (существующих и перспективных) основные функции безопасности возлагаются на компоненты ППО, однако на вычислительных узлах дополнительно используются средства защиты от НСД и антивирусные средства защиты уровня ОС средств вычислительной техники. Межсетевое

взаимодействие контролируется межсетевыми экранами, средствами обнаружения (предупреждения) вторжений и анализа защищѐнности. Каналы связи, выходящие за пределы контролируемой зоны, защищаются средствами криптографической защиты информации (шифрованной связи).

Предмет исследования настоящей выпускной квалификационной работы – разработка системы защиты информации в информационных системах персональных данных Управления Федерального казначейства по Хабаровскому краю.

Цель работы состоит в создании проекта СЗИ, в полной мере удовлетворяющей требованиям действующих нормативных правовых актов (НПА) в области защиты информации и персональных данных в частности.

Задачи:

- изучение нормативно-методических документов (НМД) в области защиты информации;

- исследование исходных данных по Управлению, включающее анализ реализованных средств защиты информации;

- разработка эффективной, удовлетворяющей всем НПА и НМД системы защиты информации.

В УФК по Хабаровскому краю реализована автоматизированная система обработки данных (АС), в состав которой входят несколько информационных систем (ИС), в том числе информационных систем персональных данных (ИСПДн).

В настоящей ВКР будут рассмотрены две ИСПДн:

- ИСПДн «АКСИОК» – ИС, предназначенная для выполнения технологических процессов работы Управления (сбор, хранение, обработка, уничтожение персональных данных сотрудников);

- ИСПДн «Конфиденциальный контур» – ИС, предназначенная для эффективного выполнения работ по обслуживанию клиентов Управления (физических лиц и бюджетных организаций).

Для создания СЗИ была разработана следующая документация:

- схемы расположения ТС относительно контролируемой зоны;
- заключения по результатам аудита ИС;
- модели угроз безопасности информации;
- акты установления уровня защищѐнности ПДн, обрабатываемых в ИС Управления;
- аналитические обоснования необходимости создания СЗИ;
- технические задания на создание СЗИ;
- технические проекты на создание СЗИ.