Приказ ФНС России от 25.02.2014 № ММВ-7-6/66@

Об утверждении Концепции системы управления информационной безопасностью ФНС России

В целях реализации пункта 6.2.6 "Концепции информационной безопасности ФНС России", утвержденной приказом ФНС России от 13.01.2012 № ММВ-7-4/6@, и повышения эффективности управления информационной безопасностью

приказываю:

1. Утвердить Концепцию системы управления информационной безопасностью ФНС России согласно приложению к настоящему приказу.

2. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Федеральной налоговой службы А.С.Петрушина.

Руководитель Федеральной
налоговой службы
М.В.Мишустин

УТВЕРЖДЕНА
приказом ФНС России
от 25 февраля 2014 года № ММВ-7-6/66@
(В редакции, введенной в действие
приказом ФНС России
от 19 июня 2018 года № ММВ-7-6/399@. -
См. предыдущую редакцию)

Концепция системы управления информационной безопасностью ФНС России

Перечень нормативных документов

1. ГОСТ Р ИСО/МЭК 27001-2013 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

2. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

3. Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных";

4. РД.ФСТЭК России. "Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры", 2007 года;

5. Приказ ФСТЭК России от 18 февраля 2013 года № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

6. Приказ ФСТЭК России от 11 февраля 2013 года № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

7. "Концепция информационной безопасности Федеральной налоговой службы", утвержденная приказом ФНС России от 13 января 2012 года № ММВ-7-4/6@;

8. "Положение по информатизации Федеральной налоговой службы", утвержденное приказом ФНС России от 23 января 2006 года № САЭ-3-13/31@;

9. "Модель угроз и нарушителя безопасности информации во внешних и внутренних каналах обмена данными АИС ФНС России"; утвержденная приказом ФНС России от 28.05.2015 № ММВ-7-6/220@;

10. "Модель угроз и нарушителя информационной безопасности объекта информатизации ФНС России", утвержденная приказом ФНС России от 23.05.2013 № ММВ-7-4/181@;

11. "Концепция построения системы управления информационной безопасностью Федеральной налоговой службы", утвержденная приказом от 10 июня 2008 года № ВЕ-4-6/24дсп@;

12. "Руководство по организации информационной безопасности на объектах информатизации Федеральной налоговой службы", утвержденное приказом от 23 октября 2007 года № ММ-4-27/29дсп@.

Обозначения и сокращения

АЦ ЦУБИ - Аналитический центр ЦУБИ;

ГИС - государственная информационная система;

ИА - информационный актив;

ИБ - информационная безопасность;

ИКД - информационная карточка документов;

ИКСИБ - информационная карточка сотрудника ИБ;

ИКТС - информационная карточка третьей стороны;

ИКИ - информационная карта инцидентов;

ИКР - информационная карта рисков;

ИТ - информационные технологии;

КИИ - критическая информационная инфраструктура;

ИЛП ОИ - Информационно-логический паспорт объекта информатизации;

МИ ФНС России по ЦОД - Межрегиональная инспекция ФНС России по централизованной обработке данных;

МИ ФНС России по КН - Межрегиональная инспекция ФНС России по крупнейшим налогоплательщикам;

МИ ФНС России по ФО - Межрегиональная инспекция ФНС России по Федеральному округу;

СМЭВ - Система межведомственного электронного взаимодействия.

СОБИ ФНС России - Система обеспечения безопасности информации ФНС России;

СУИБ - Система управления информационной безопасностью;

ТОРМ ФНС России - Территориально-обособленное рабочее место ФНС России.

ПДн - персональные данные;

ПО - программное обеспечение;

МЭДО - Межведомственный Электронный Документооборот;

ТС - техническое средство;

УФНС России - Управление ФНС России по субъекту Российской Федерации;

ФКУ ФНС России - Федеральное казенное учреждение "Налог-Сервис" ФНС России;

ЦУБИ ФНС России - Центр управления безопасностью информации ФНС России.

1. Общие положения

Настоящая концепция управления информационной безопасностью (ИБ) определяет систему взглядов на проблему регулирования и координации при управлении информационной безопасностью в Федеральной налоговой службе, ее территориальных органах и подведомственных организациях, а также при взаимодействии налоговых органов между собой, с Федеральными органами государственной власти и при оказании государственных услуг.

Под управлением информационной безопасностью в ФНС России понимается подмножество взаимоувязанных, циклических процессов, направленных на достижение заданных параметров ИБ.

Под системой управления информационной безопасностью (СУИБ) в ФНС России понимается часть общей системы управления, основанной на оценке рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

СУИБ ФНС России включает в себя политики, действия по планированию, распределение ответственности, практики, процедуры, процессы и ресурсы.

Создание централизованной СУИБ является стратегическим решением ФНС России.

Целями создания СУИБ ФНС России являются:

- повышение доверия к ФНС России со стороны граждан Российской Федерации;

- повышение стабильности функционирования отдельных налоговых органов и, как следствие, всей Службы в целом;

- предотвращение и/или снижение до приемлемого уровня ущерба от инцидентов ИБ;

- снижение затрат на ИБ в ФНС России за счет оптимизации СУИБ;

- достижение адекватности мер по защите в зависимости от реальности угроз ИБ и допустимых рисков;

- информационная поддержка 8-го Центра ФСБ России по вопросам сетевых атак на ресурсы АИС ФНС России;

- информационная поддержка служб собственной безопасности при обеспечении превентивных мер и проведении расследований.

Основными задачами СУИБ ФНС являются:

- управление политиками информационной безопасности и поддержание документации информационной безопасности в актуальном состоянии;

- управление угрозами информационной безопасности и рисками;

- управление активами информационной безопасности и поддержание информационной безопасности в актуальном состоянии;

- управление персоналом информационной безопасности и организациями-подрядчиками;

- управление процессами информационного обеспечения подразделений собственной безопасности налоговых органов и "специальными" вопросами;

- управление инцидентами информационной безопасности;

- управление системой криптографической защиты информации;

- оперативное управление и мониторинг состояния информационной безопасности в налоговых органах;

- техническое сопровождение и эксплуатация средств СОБИ

Решение задач управления организуется и обеспечивается центром управления безопасностью информации ФНС России.

Под Центром управления безопасностью информации (ЦУБИ) ФНС России понимается организационно-функциональная структура ЦА ФНС России и подчиненного ему аналитического центра (АЦ).

Под филиалами ЦУБИ понимаются подразделения ИБ в составе УФНС России и Межрегиональных инспекций ФНС России.

Вопросы управления информационной безопасностью тесно взаимоувязаны с вопросами управления ИТ структурой и собственной безопасностью. Средства автоматизированной поддержки управления ИБ и ИТ структурой могут строиться

на базе единой платформы. Вместе с тем управление ИБ имеет свою специфику и должно организовываться как самостоятельная и независимая система.

Действующие нормативные документы по ИБ определяют необходимость построения СУИБ и, как следствие, ЦУБИ как самостоятельной системы.

Процесс управления ИБ в ФНС России организуется с помощью множества правил, представляющих сложную иерархическую систему технологических, инструктивных и организационно-распорядительных документов, предназначенных для исполнения различными категориями сотрудников ФНС России. Совокупность таких правил формирует Политику управления ИБ в ФНС России. Концепция СУИБ является документом общей Политики ИБ ФНС России, отражающей официально принятую в ФНС России систему взглядов на СУИБ и пути ее решения.

Концепция СУИБ определяет пути достижения требуемого уровня управления ИБ (при проектировании и внедрении, обеспечении функционирования (эксплуатации) и контроле) в ходе оказания государственных информационных услуг и при повседневной деятельности подразделений ФНС России через создание продуманной, централизованной системы управления ИБ.

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

Внутренние документы ФНС России по управлению, затрагивающие вопросы ИБ, должны разрабатываться с учетом положений Концепции СУИБ и не противоречить им.

Настоящая Концепция определяет основные принципы построения СУИБ и ЦУБИ с точки зрения реализации единой политики ИБ ФНС России.

В первом разделе приведено общее описание структуры СУИБ, определено место ЦУБИ в этой структуре.

Во втором разделе концепции определяются процессы регулирования при управлении информационной безопасностью. Приводится описание каждого из процессов в обобщенном виде.

В третьем разделе концепции представлено описание функций ЦУБИ, являющегося механизмом реализации эффективного управления ИБ в ФНС России. Для информационной поддержки ЦУБИ создается аналитический центр ФНС России. В разделе определены основные функции и задачи автоматизированной поддержки СУИБ.

В четвертом разделе схематично определена обобщенная организационно-функциональная структура ЦУБИ и аналитического центра, а также определены основные функции филиала ЦУБИ в УФНС России или МИ ФНС России по КН.

2. Процессы регулирования при управлении информационной безопасностью

Общая схема взаимодействия процессов регулирования при управлении ИБ представлена на рис.1.

Представленная на рис. 1 схема соответствует модели PDCA международного стандарта ИСО/МЭК 27001-2013 г.

Процессы регулирования при управлении ИБ включают в себя:

- разработку политик и требований к ИБ;

- разработку и внедрение СУИБ ФНС России;

- обеспечение функционирования (эксплуатацию) СУИБ;

- контроль состояния ИБ.

СУИБ разрабатывается в ФНС России с учетом требований и политик в области ИБ. Взаимоувязанные процессы управления ИБ в ФНС России должны обеспечить централизованно управляемую систему информационной безопасности.

Внедрение средств и систем СУИБ организуется ФНС России.

Внедрение СУИБ осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

- установку и настройку средств СУИБ;

- разработку документов, определяющих правила и процедуры, реализуемые эксплуатирующими подразделениями для обеспечения СУИБ;

- внедрение организационных мер защиты информации;

- предварительные испытания СУИБ;

- опытную эксплуатацию СУИБ;

- анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

- приемочные испытания СУИБ.

Проверка работоспособности СУИБ проводится на этапах внутренних испытаний и опытной эксплуатации комиссиями в составе представителей подрядчиков и заказчика.

Обеспечение функционирования и эксплуатация готовых средств и систем СУИБ должна производиться Центром управления безопасностью информации и назначенными сотрудниками налоговых органов. Оперативная поддержка задач эксплуатации осуществляется АЦ, входящим в состав ЦУБИ. Технологические процессы эксплуатации должны быть обеспечены соответствующей документальной поддержкой.

Обеспечение функционирования (эксплуатации) СУИБ на региональном уровне производится сотрудниками на основании должностных регламентов или приказов.

Эксплуатация технико-программных средств ЦУБИ осуществляется сотрудниками аналитического центра ЦУБИ.

Контроль управления безопасностью информации ФНС России осуществляется постоянно руководством соответствующего уровня. Высшим звеном контроля, в соответствии с требованиями Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам" (утв. Постановлением Совета Министров - Правительства РФ от 15.09.1993 № 912-51), является руководитель ФНС России.

Основные функции контроля исполняются в рамках функционирования СУИБ. Работы по контролю управления безопасностью информации ФНС России организуются ЦУБИ ФНС России. При организации мероприятий контроля используются данные, полученные в АЦ ЦУБИ.

Контроль функционирования системы управления ИБ в ФНС России является составной частью общей системы контроля ИБ в ФНС России. Контроль ИБ в ФНС России подразделяется на внешний и внутренний.

Внешний контроль проводится государственными регуляторами в области ИБ (ФСБ России, ФСТЭК России и Роскомнадзор) по собственным планам, согласованным с ФНС России на основании собственных нормативных документов.

Внутренний контроль (в том числе дистанционный контроль) проводится:

- ЦУБИ по отдельному плану, согласованному с проверяемыми подразделениями, на основании введенной приказом ФНС России методики, а также в рамках функционирования СУИБ;

- МИ ФНС России по ФО по отдельным планам проверки основных видов деятельности ФНС России или тематических планов по виду деятельности, согласованными с проверяемыми подразделениями, на основании регламента, введенного приказом ФНС России;

- УФНС России внутри и в подчиненных ИФНС России и ТОРМ ФНС России по отдельным планам;

- МИ ФНС России по КН внутри по отдельным планам.

Взаимоувязанные процессы регулирования управления ИБ в ФНС России позволяют на основании сформулированных требований в области управления иметь адекватную централизованную управляемую информационную безопасность ФНС России.

Рисунок 1

3. Функции ЦУБИ

Общая схема организационно-функциональной структуры ЦУБИ ФНС России представлена на рис. 2.

Под ЦУБИ ФНС России понимается организационно-функциональная структура, реализующая цели управления информационной безопасностью ФНС России.

Основные направления деятельности и обобщенная организационно-функциональная структура ЦУБИ представлены в Разделе 4 данного документа.

Структура ЦУБИ представлена в виде ядра (аналитического центра) и перечня сегментов, которые и составляют элементную базу ЦУБИ. Описание каждого элемента ЦУБИ включает описание предметной области и выходного результата.

3.1. Аналитический центр ЦУБИ

Аналитический центр является организационно-функциональной структурой в составе ЦУБИ и обеспечивает информационную поддержку ЦУБИ и оперативный мониторинг состояния ИБ ФНС России.

Технологическая компонента поддержки функционирования аналитического центра представляет собой систему автоматизированной информационной поддержки управления ИБ (САПУИБ) и включает:

- технологический модуль интерфейса взаимодействия системы обеспечения безопасности информации (СОБИ) и ЦУБИ;

- технологический модуль ввода и обработки данных о состоянии ИБ;

- подсистема управления и учета активов;

- подсистема предоставления информации;

- подсистема обеспечения ИБ САПУИБ;

- подсистема управления инцидентами ИБ;

- подсистема управления рисками ИБ;

- подсистема контроля соответствия требованиями.

Выходные формы технологической компоненты поддержки функционирования ЦУБИ представляются по любому из элементов, составляющих СУИБ ФНС России (приложение № 1).

3.2. Задачи системы управления информационной безопасностью в ФНС России

3.2.1. Управление политиками ИБ и поддержание документации в актуальном состоянии

Управление политиками ИБ подразумевает:

- анализ развития нормативных правовых актов Российской Федерации по вопросам ИБ;

- анализ мировых и российских тенденций развития систем, средств и мер, обеспечивающих ИБ;

- разработку стратегической линии развития ИБ в ФНС России;

- разработку нормативной базы политик ИБ в ФНС России;

- доведение политик ИБ ФНС России до всех подразделений ФНС России и подведомственных подразделений.

Результатами работ данного сегмента СУИБ является актуальный комплект нормативных документов, определяющих политики ИБ на каждый момент времени.

Автоматизированная поддержка данного сегмента СУИБ включает:

- ввод и хранение информационных карточек документов (ИКД).

- формирование ИКД, структурированных по 4-м типам каталогов:

- нормативные правовые акты государственных регуляторов в области ИБ);

- Постановления Правительства;

- нормативные документы ФНС России;

- методические и инструктивные документы ФНС России;

- рабочие документы подразделений ИБ.

- формирование каталога Интернет-ресурсов по тематике ИБ;

- формирование новостных сообщений для пользователей ЦУБИ;

- информационное взаимодействие пользователей ЦУБИ посредством форума.

- вывод информационных панелей для уведомления:

- о количестве документов, требующих актуализации (пересмотра);

- о количестве документов с различными статусами по типам каталогов.

По данному направлению в филиалах ЦУБИ осуществляется сопровождение актуального комплекта нормативных документов по вопросам ИБ.

3.2.2. Управление угрозами ИБ и рисками

Моделирование угроз для объектов ФНС России проводится исходя из требований регуляторов, предъявляемых к автоматизированной системе ФНС России, как системе, причисляемой к:

- критическим информационным инфраструктурам (КИИ);

- Государственным информационным системам (ГИС);

- системам, обрабатывающим персональные данные (ПДн);

- крупным телекоммуникационным системам, для защиты каналов которых используются криптографические средства защиты;

- системам, входящим в СМЭВ и МЭДО.

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

В рамках данного сегмента СУИБ проводится оценка возможных рисков при реализации той или иной угрозы ИБ, выявляются наиболее критичные с точки зрения ИБ узлы системы.

Основными функциями управления угрозами и рисками являются:

- разработка и сопровождение перечней потенциальных угроз и возможностей нарушителей ИБ, с учетом требований ИБ КИИ, ГИС, ПДн, телекоммуникационным системам, СМЭВ, МЭДО и защиты сайтов;

- анализ и использование в процессах моделирования методологий регуляторов (ФСБ России и ФСТЭК России) по указанным направлениям;

- формирование пороговых значений рисков при реализации возможных угроз ИБ;

- определение уровня необходимой защиты объектов с учетом возможных рисков;

- доведение и разъяснение положений моделей угроз и нарушителей и уровней необходимой защиты до подразделений ФНС России и приданных подразделений.

Результатами работ данного сегмента СУИБ являются актуальные модели угроз и нарушителей ИБ в каждый момент времени и рассчитанные уровни ИБ с учетом рисков.

Автоматизированная поддержка данного сегмента СУИБ включает:

- формирование справочника угроз ИБ с возможностью актуализации;

- формирование справочника уязвимостей ИБ с возможностью актуализации;

- формирование информационных карт рисков (ИКР):

- установление пороговых значений для атрибутов, влияющих на определение величины рисков (предусматривается несколько градаций);

- определение уровня рисков.

- предложение способов обработки рисков;

- формирование перечня защитных мер;

- оценка остаточных рисков;

- вывод информационных панелей для уведомления:

- о количестве рисков для систем с разными уровнями;

- о необходимости переоценки рисков;

- о новых угрозах и возможностях потенциальных нарушителей;

- о результатах моделирования "риск-противодействие-оценка целесообразности".

По данному направлению в филиалах ЦУБИ выполняются следующие работы:

- анализ возможно имеющихся "специфичных" для конкретного объекта угроз;

- анализ возможно имеющихся специфичных рисков и их оценка.

3.2.3. Управление активами ИБ и поддержание ИБ в актуальном состоянии

Под активами ИБ ФНС России будем понимать информационные, программные и технические ресурсы, которые могут потерять частично или полностью свойства ИБ (конфиденциальность, доступность или целостность) при реализации угроз.

Классификация активов ИБ подразумевает как классификацию систем с точки зрения защиты от угроз нарушения конфиденциальности, так и классификацию с точки зрения доступности и целостности информации, которые рассматриваются в качестве основных характеристик надежности технико-программных средств и технологических систем.

Классификация активов ИБ подразумевает также определение критичности того или иного средства или системы с точки зрения ИБ. Процессы управление критичными с точки зрения ИБ активами пересекаются с процессами управления ИТ структурой.

Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - третий, самый высокий - первый.

Класс защищенности информационной системы подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации информационной системы оформляются актом классификации.

Поддержание активов ИБ в актуальном состоянии предполагает также поддержку оценивания достаточности мер и средств ИБ, а также построение моделей зрелости СУИБ.

Основными функциями определения и классификации активов ИБ и поддержания их в актуальном состоянии являются:

- учет имеющихся на объекте технических, программных средств и технологий, критичных с точки зрения ИБ, включая средства и технологии СУИБ;

- учет защищаемой информации;

- сопровождение внешних аудитов ИБ;

- организация и проведение внутренних аудитов;

- анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании систем защиты информации информационной системы;

- контроль защищенности информации, содержащейся в информационной системе;

- определение эффективности и достаточности существующей системы ИБ и выработка предложений по совершенствованию;

- построение и сопровождение модели зрелости СУИБ.

Результатами работ данного сегмента СУИБ являются перечни параметров критичных с точки зрения ИБ, таблицы соответствия требованиям ИБ и модели зрелости СУИБ на каждом объекте информатизации в любой момент времени.

Общий порядок контроля (в том числе дистанционного контроля) соответствия активов ИБ требованиям безопасности (проведение аудитов ИБ) представлен в разделе 2 настоящего документа.

Автоматизированная поддержка данного сегмента СУИБ включает:

- формирование справочника технических средств, критичных с точки зрения ИБ, содержащего описание ТС и информацию, определяющую критичность;

- формирование справочника программного обеспечения, критичного с точки зрения ИБ, содержащего описание ПО и информацию, определяющую критичность;

- формирование справочника информационных активов (ИА), содержащего описание ИА, сведения о наличии информации, составляющей налоговую тайну и информацию, необходимую для определения критичности ИА с точки зрения ИБ;

- формирование справочников аудитов ИБ и основных результатов их проведения;

- формирование информационных карточек требований ИБ, содержащих опросные листы, позволяющих определить степень их выполнения;

- формирование иерархической структуры показателей оценки выполнения требований по различным направлениям обеспечения ИБ;

- формирование коэффициентов значимости (критичности) показателей (весовые коэффициенты);

- формирование информационно-логических паспортов объектов информатизации ФНС России (ИЛП ОИ). В ИЛП ОИ должна содержаться информация в соответствии с требованиями нормативных актов по ИБ;

- определение уровня безопасности в зависимости от:

- данных опросных листов;

- определения уровня критичности ИА, ТС и ПО, входящих в состав ЛП ИСО.

- формирование реестра информационных ресурсов;

- построение моделей "зрелости" СУИБ на основании данных по критичности;

- вывод информационных панелей для уведомления:

- о ТС, ПО, и ИА с высоким уровнем критичности по ИБ;

- об информации, составляющей налоговую тайну;

- об уровнях соответствия требованиям ИБ;

- о необходимости проведения очередной оценки соответствия;

- о данных по "зрелости" СУИБ;

- о ландшафте ИБ АИС ФНС России.

- формирование реестров объектов с замечаниями по результатам аудитов (в том числе дистанционных) и отметках по устранению замечаний.

По данному направлению филиалы ЦУБИ выполняют следующие работы:

- проведение аудита (в том числе дистанционного) по ИБ в подчиненных ИФНС России и ТОРМ ФНС России;

- заполнение анкет по вопросам ИБ и ввод данных анкет в информационную систему ЦУБИ, формирование отчетности по вопросам ИБ;

- установка средств защиты информации;

- эксплуатация и поддержание в работоспособном состоянии средств защиты информации;

- контроль работы пользователей в системе:

- правильности входа в систему и целостности (с использованием средств двухфакторной аутентификации);

- контроль трафика, печати документов и копирования на внешние носители (с использованием средств предотвращения утечек информации);

- поддержание в рабочем состоянии справочников технических средств, программного обеспечения и информационных ресурсов, критичных с точки зрения ИБ;

- формирование и ведение информационно-логических паспортов объекта;

- контроль исполнения указаний вышестоящих инстанций по вопросам ИБ.

3.2.4. Управление персоналом и подрядчиками работ по ИБ

Управление персоналом ФНС России, занятым в области ИБ, включает в себя кадровые вопросы и обучение персонала вопросам ИБ. Вопрос квалификации персонала ИБ, является одним из ключевых при определении уровня зрелости СУИБ объекта информатизации.

При управлении работами с подрядчиками разрабатывающими, внедряющими, поставляющими, или ремонтирующими средства и системы защиты следует в обязательном порядке учитывать вопросы ИБ. Кадровая работа с сотрудниками, участвующими в процессе управления ИБ в обязательном порядке включает вопросы контроля допуска к налоговой тайне.

При работе с подрядчиками следует учитывать уровень обеспечения ИБ в подрядных организациях.

Основными функциями управления персоналом и подрядчиками являются:

- организация централизованной схемы управления по схеме: руководство ФНС России - ЦУБИ - руководство УФНС России (МИ ФНС России по КН);

- сокращение затрат за счет удаления функций управления ИБ из звена ИФНС России;

- организация подбора квалифицированного персонала;

- организация обучения вопросам ИБ;

- организация и проведение работ по государственным контрактам.

Результатами работ данного сегмента ЦУБИ является квалифицированный персонал ИБ ФНС России и исполнение государственных контрактов в заданные сроки.

Автоматизация данного сегмента СУИБ включает:

- ввод и хранение информационных карточек сотрудников ИБ (ИКСИБ).

- информирование и тестирование персонала по вопросам ИБ.

- ввод и хранение информационных карточек третьих сторон (ИКТС):

- контрагентов;

- государственных органов, с которыми осуществляется взаимодействие ФНС России;

- ассоциаций и профессиональных групп в области ИБ, с которыми осуществляется взаимодействие ФНС России;

- ввод и хранение информационных карточек о работах по государственным контрактам:

- о сроках работ по государственным контрактам;

- о количестве и месте установки технико-программных средств ИБ.

- вывод информационных панелей для уведомления:

- о результатах тестирования персонала;

- о сроках действия различных соглашений и договоров.

По данному направлению филиалы ЦУБИ выполняют следующие работы:

- управление персоналом ИБ территориального органа;

- участие в семинарах и конференциях по вопросам ИБ;

- учеба на курсах, семинарах и дистанционно по вопросам ИБ.

3.2.5. Управление процессами информационного обеспечения собственной безопасности и "специальными вопросами" ИБ

Управление процессами информационного обеспечения собственной безопасности включает три направления:

- обеспечение информацией комиссий при разборе инцидентов собственной безопасности;

- текущая работа по информационному обеспечению для организации превентивных мер собственной безопасности, в том числе для защиты особо ценной информации и выявлению инцидентов ИБ;

- специальные вопросы ИБ, связанные с защитой государственной тайны.

Основными функциями управления процессами информационного обеспечения собственной безопасности, в том числе в филиалах ЦУБИ (в части их касающейся), являются:

- информационное обеспечение для превентивных мер по защите особо ценной информации, находящейся в ФНС России и организация защиты этой информации в АИС ФНС России;

- формирование совместно с сотрудниками ЦА ФНС России перечней злонамеренных действий в информационной системе ФНС России, указывающих на попытку организации инцидента собственной безопасности;

- инициализация расследований собственной безопасности по результатам анализа действий в АИС ФНС России, указывающих на попытку или совершение инцидентов собственной безопасности;

- обеспечение информацией служб собственной безопасности при проведении расследований и локализации последствий нарушений безопасности;

- обеспечение конфиденциальности информации в отношении охраняемых лиц;

- представление информации внешним уполномоченным органам при проведении расследований;

- организация расследований по тематике ИБ;

- организация спецсвязи для высших должностных лиц ФНС России;

- организация проведения аттестаций помещений и АРМ;

- мониторинг активности радиоэфира с целью обнаружения средств съема информации.

Для информационного обеспечения собственной безопасности используются данные подсистем в составе СОБИ и иная информация.

По заданиям руководства ФНС России могут проводиться мероприятия анализа выделенных массивов и систем на предмет возможных нарушений безопасности.

Результатами работ данного сегмента СУИБ является информационное обеспечение собственной безопасности для организации превентивных мер и расследований.

Автоматизация данного сегмента СУИБ подразумевает:

- ведение локальных баз данных с особо ценной информацией;

- ведение баз данных с результатами работы группы и подразделений собственной безопасности на выделенных, изолированных от АИС "Налог-3" ресурсах.

3.2.6. Управление инцидентами ИБ

Управление инцидентами ИБ заключается в:

- подготовке и описании через корреляционные взаимозависимости элементарных событий ИБ;

- обнаружении и идентификации инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- своевременной передаче сведений в ЦУБИ при появлении "значимых" инцидентов ИБ на том или ином технологическом участке;

- анализе инцидентов, в том числе определении источников и причин возникновения инцидентов, а также оценки их последствий;

- планировании и принятии мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрению вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планировании и принятии мер по предотвращению повторного возникновения инцидентов.

ЦУБИ ФНС России анализирует отчеты по инцидентам ИБ и проводит расследования. Результатами работ данного сегмента СУИБ являются управляемая с точки зрения инцидентов ИБ и достаточности мер ИБ в каждый момент времени система безопасности.

Автоматизированная поддержка данного сегмента СУИБ, в том числе в филиалах ЦУБИ (в части их касающейся), включает:

- Создание информационных карт по инцидентам ИБ (ИКИ) и состоянию ИБ для объектов ФНС России;

- Накопление и обработка данных об инцидентах ИБ и состоянии ИБ;

- Учет привлекаемых должностных лиц, проводимых мероприятий и результатов их выполнения, а также принятых решений в процессе обработки инцидентов ИБ;

- Рассылку уведомлений заинтересованным лицам об инцидентах ИБ;

- Формирование отчетов по результатам расследований инцидентов ИБ и состоянию ИБ;

- Вывод информационных панелей с данными:

- о количестве инцидентов ИБ по статусу обработки;

- о количестве инцидентов ИБ по типам;

- о лицах для уведомления об инцидентах ИБ;

- о ландшафте ИБ АИС ФНС России.

3.2.7. Управление системой криптографической защиты информации

Управление системой криптографической защиты информации (СКЗИ) включает в себя:

- организацию деятельности и развитие Удостоверяющего Центра (УЦ) ФНС России;

- организацию ведомственного надзора за использованием СКЗИ;

- организацию работ в ФНС России по использованию электронной подписи при работе с налогоплательщиками, при межведомственном электронном документообороте, а также при взаимодействии в рамках договоров с иностранными государствами;

- организацию работ по сертификации средств СКЗИ.

Работы по моделированию системы защиты и анализу угроз информации при передаче по телекоммуникационным каналам, а также нормативно-техническое сопровождение работ СКЗИ проводятся в рамках управления соответствующими сегментами СУИБ (см. пп.3.2.1., 3.2.2).

Результатами работ данного сегмента СУИБ является СКЗИ, удовлетворяющая требованиям законодательства Российской Федерации.

Автоматизированная поддержка данного сегмента СУИБ, в том числе в филиалах ЦУБИ (в части их касающейся), включает:

- накопление и обработку данных о состоянии СКЗИ;

- функционирующего в штатном режиме УЦ ФНС России;

- накопление и обработку данных о сертификатах СКЗИ.

3.2.8. Оперативное управление и мониторинг состояния ИБ

Оперативное управление и мониторинг состояния ИБ заключаются в:

- контроле за событиями безопасности и действиями пользователей в информационной системе;

- предотвращение нежелательной сетевой активности и вторжений;

- контроле доступности и целостности СОБИ;

- документирование процедур и результатов мониторинга состояния ИБ;

- принятие решения по результатам мониторинга состояния ИБ.

В силу значительной стоимости систем оперативного мониторинга инцидентов ИБ, их установка может производиться поэтапно исходя из значимости объектов внедрения.

Результатами работ данного сегмента СУИБ являются оперативное отражение различных атак на информационную систему ФНС России и постоянный контроль целостности средств СОБИ.

Автоматизированная поддержка данного сегмента СУИБ включает:

- Создание информационных карт по результатам мониторинга состояния ИБ (ИКИ);

- Обработка данных о результатах мониторинга состояния ИБ;

- Учет привлекаемых должностных лиц, проводимых мероприятий и результатов их выполнения, а также принятых решений в процессе обработки инцидентов ИБ;

- Формирование отчетов по результатам расследований инцидентов ИБ и состоянию ИБ;

- Вывод информационных панелей с данными:

- о количестве инцидентов ИБ по статусу обработки, выявленных в результате мониторинга;

- о количестве инцидентов ИБ по типам, выявленных в результате мониторинга;

- о лицах для уведомления о событиях мониторинга ИБ.

По данному направлению филиалы ЦУБИ выполняют следующие работы:

- мониторинг исполнения политик ИБ и целостности средств защиты.

4. Основные задачи и организационно-функциональная структура ЦУБИ

Основные направления деятельности ЦУБИ включают:

- определение политик ИБ и нормативно-техническое обеспечение;

- работа с персоналом ИБ и с подрядчиками;

- управление СКЗИ;

- контроль состояния ИБ и расследование инцидентов;

- обеспечение "специальных вопросов" безопасности на объектах информатизации ФНС России;

- управление аналитическим центром ЦУБИ.

Основные направления деятельности по эксплуатации ИБ в сегментах УФНС России и МИ ФНС России по КН частично и в меньшем масштабе аналогичны вопросам, решаемым ЦУБИ на уровне системы в целом.

4.1. Задачи определения политик ИБ и нормативно-технического обеспечения

- Своевременное и полное выявление тенденций, угроз и факторов риска безопасности информации в ФНС России.

- Взаимодействие с государственными регуляторами в области ИБ.

- Анализ текущего состояния и развития вопросов ИБ в РФ и подготовка изменений в нормы и правила ИБ для ФНС России, актуализация нормативных и организационно-распорядительных документов в ФНС России.

- Анализ актуальных угроз ИБ и статистики реальных инцидентов безопасности.

- Поддержание в актуальном состоянии моделей угроз ИБ ФНС России.

- Реализация специальных проектов ФНС России по защите информации, в том числе, по комплексу инженерно-технических мер.

4.2. Задачи управления персоналом ИБ и подрядчиками

- Сопровождение работ по государственным контрактам.

- Организация обучения вопросам ИБ сотрудников ФНС России.

- Организация закупок технико-программных средств.

4.3. Задачи управления СКЗИ

- Методологические и организационные задачи применения электронной подписи при межведомственном обмене и при электронном обмене с налогоплательщиками.

- Координация и контроль за деятельностью региональных центров сертификации.

- Оказание методологической поддержки в части применения СКЗИ.

- Контроль за соблюдением условий использования СКЗИ.

- Организация обмена информацией с иностранными государствами.

- Организация работ с сертификатами СКЗИ.

- Организация работ по устранению замечаний внешнего аудита ФСБ России.

- Организация работ УЦ.

4.4. Задачи контроля состояния ИБ и расследования инцидентов

- Аналитическая работа по анализу состояния ИБ.

- Определение и классификация активов ИБ, поддержание их в актуальном состоянии.

- Организация и проведение аудитов ИБ в ФНС России.

- Анализ результатов аудитов, проводимых силами МИ ФНС России по ФО и УФНС России.

- Организация и проведение расследований инцидентов ИБ.

- Сопровождение перечня актуальных инцидентов ИБ.

- Организация работ по устранению замечаний внешнего аудита.

- Координация действий по эксплуатации СУИБ.

4.5. Задачи обеспечения "специальных вопросов" ИБ

- Разработка специальных мер ИБ для "особо ценной" информации.

- Исполнение указаний руководства ФНС России по "специальным" вопросам.

- Предоставление информации в службу собственной безопасности для организации превентивных мер защиты.

- Предоставление информации по запросу службы собственной безопасности при проведении расследований.

- Обеспечение конфиденциальности информации в отношении охраняемых лиц.

- Организация расследований по тематике ИБ.

- Мониторинг активности радиоэфира с целью обнаружения средств съема информации.

- Организация спецсвязи для высших должностных лиц ФНС России.

- Организация проведения аттестаций помещений и АРМ в ФНС России.

4.6. Задачи управления аналитическим центром ИБ

- Сопровождение СОБИ и САПУИБ.

- Подготовка отчетов о состоянии ИБ в ФНС России.

- Подготовка материалов и отчетов об инцидентах

- Сопровождение таблиц актуальных и текущих инцидентов ИБ.

- Взаимодействие с сотрудниками ИБ на местах по вопросам информационной поддержки.

- Мониторинг доступности и целостности СОБИ.

- Мониторинг и оперативное отражение вторжений в систему.

Обобщенная организационно-функциональная структура ЦУБИ представлена на схеме (приложение № 2).

Приложение № 1

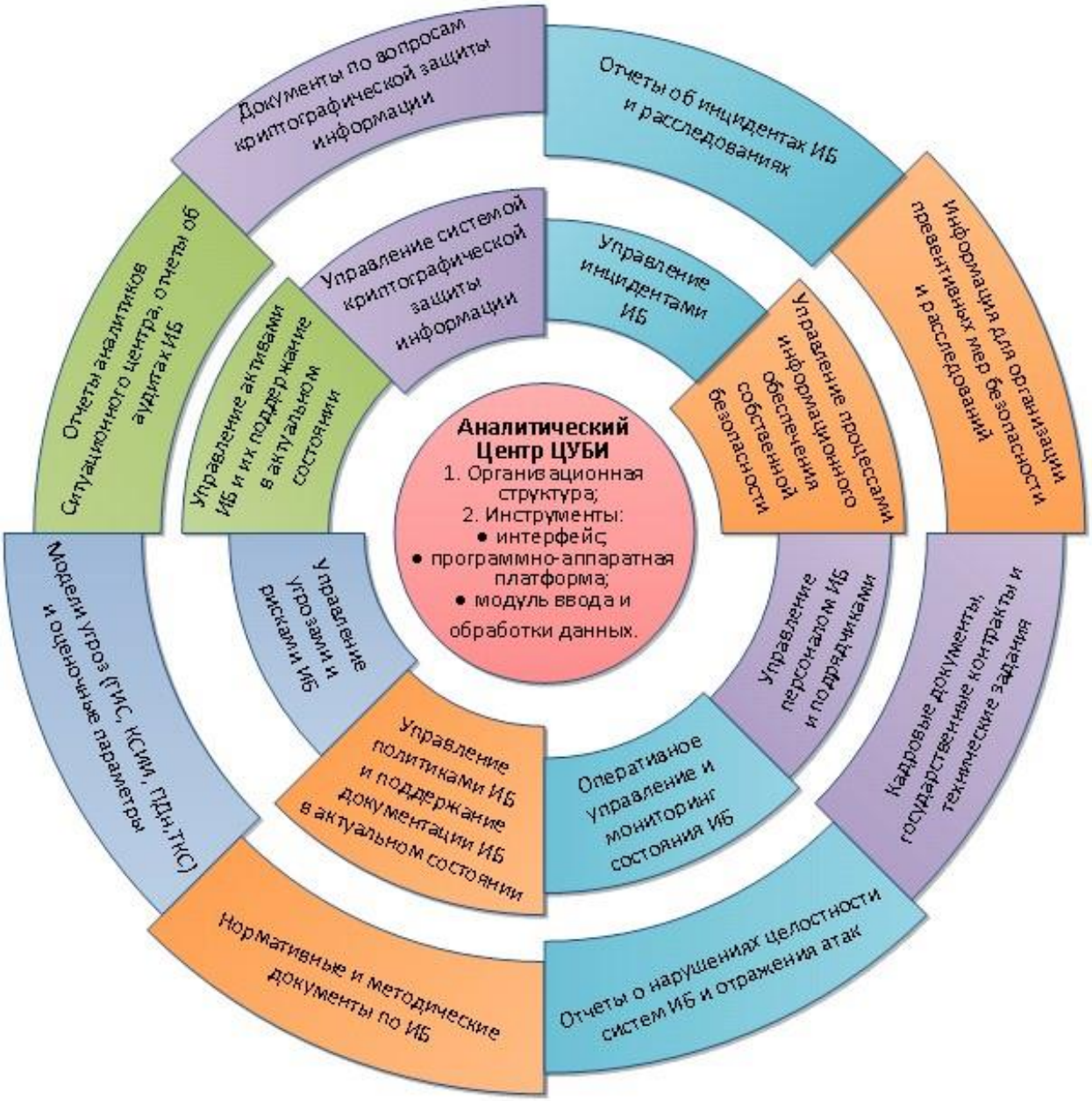
к Концепции системы управления

информационной безопасностью ФНС России

утвержденной приказом ФНС России

от "__" _____ 2018 года N ____

Приложение 1. Функциональная схема ЦУБИ



Приложение № 2

к Концепции системы управления

информационной безопасностью ФНС России

утвержденной приказом ФНС России

от "__" _____ 2018 года N ____

Приложение 2. Организационно-функциональная структура ЦУБИ