Соблюдение законодательства Российской Федерации в области защиты персональных данных в МЧС России

Блохин Сергей Михайлович,
начальник отдела организации функционирования защищенных информационно-телекоммуникационных технологий Управления информационных технологий и связи МЧС России, полковник внутренней службы

В Доктрине информационной безопасности Российской Федерации задача защиты информационных ресурсов, информационных и телекоммуникационных систем, определена как одна из актуальнейших составляющих национальных интересов Российской Федерации. На систему информационной безопасности возлагаются задачи по организации защиты и предотвращению ущерба, который может быть нанесен за счет хищения, разглашения, утечки, утраты, искажения и уничтожения информации.

Информационная безопасность — это, прежде всего, отсутствие информационных угроз, или состояние защищенности и, следовательно, устойчивости основных сфер человеческой деятельности по отношению к возможным опасным информационным воздействиям[1].

Стоит отметить, что методологические основы обеспечения информационной безопасности в большинстве случаев являются общеприменительными, независимо от формы собственности и способов управления организацией.

Областью использования системы защиты персональных данных являются следующие информационные системы МЧС России:

- автоматизированная информационно-управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (АИУС РСЧС);
- система вызова экстренных оперативных служб по единому номеру «Система-112»;
- ИС «Делопроизводство»;
- АИС «Монолит»;
- сегменты СМЭВ и МЭДО МЧС России.

В рамках федеральной целевой программы «Пожарная безопасность в Российской Федерации на период до 2017 года», утвержденной постановлением Правительства Российской Федерации от 30.12.2012 №1481, в МЧС России продолжают проводиться мероприятия по созданию системы безопасности связи в главных управлениях МЧС России и на объектах подразделений федеральной противопожарной службы. Объектовые комплексы безопасности связи предназначены для обеспечения защиты информационных ресурсов, в том числе персональных данных (далее ПДн) в информационных системах МЧС России (рис.1).

Для достижения требуемого уровня защищенности информационных систем, оперативного реагирования на возникающие угрозы и негативные тенденции в МЧС России применяется комплекс мер и средств, направленных на выявление, противодействие и ликвидацию различных угроз безопасности информации, в том числе ПДн.

В соответствии с федеральным законом №152 от 27 июля 2006 года «О персональных данных» МЧС России, как оператор персональных данных, обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Правительство Российской Федерации в постановлении от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливает:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

В соответствии с совместным приказом ФСТЭК России, ФСБ России, Минкомсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», каждая информационная система подлежит классификации. В результате классификации определяются характеристики информационной системы, затем ей присваивается класс. Для каждого класса установлены требования к функциональности по обеспечению безопасности данных.

Для решения задач подсистемы обеспечения информационной безопасности должен быть предусмотрен соответствующий комплекс программно-технических средств и организационных (процедурных) решений по защите информации от несанкционированного доступа.

Основными задачами, возлагаемыми на технические средства защиты информации МЧС России, являются:

- разграничение доступа к информации, в том числе к персональным ПДн, АС МЧС России на основе установленных правил разграничения доступа;
- защита серверов, автоматизированных рабочих мест и телекоммуникационного оборудования от несанкционированного доступа к их ресурсам;

1 Тонконогов А. В. Информационно-психологическая безопасность в системе духовной безопасности современной России. Журнал Власть 2010 №6. С. 53–56.

Состав типового комплекса:

1. Модуль межсетевого экранирования
2. Модуль обнаружения сетевых атак
3. Модуль криптографической защиты трафика
4. Модуль защиты серверов и рабочих станций – сервера и АРМ со специальным программным обеспечением
5. Модуль разграничения доступа к активному сетевому оборудованию
6. Модуль управления событиями информационной безопасности
7. Модуль контроля защищенности – Ноутбук со специальным программным обеспечением (на схеме не представлен)

СХЕМА типового комплекса системы безопасности связи МЧС России

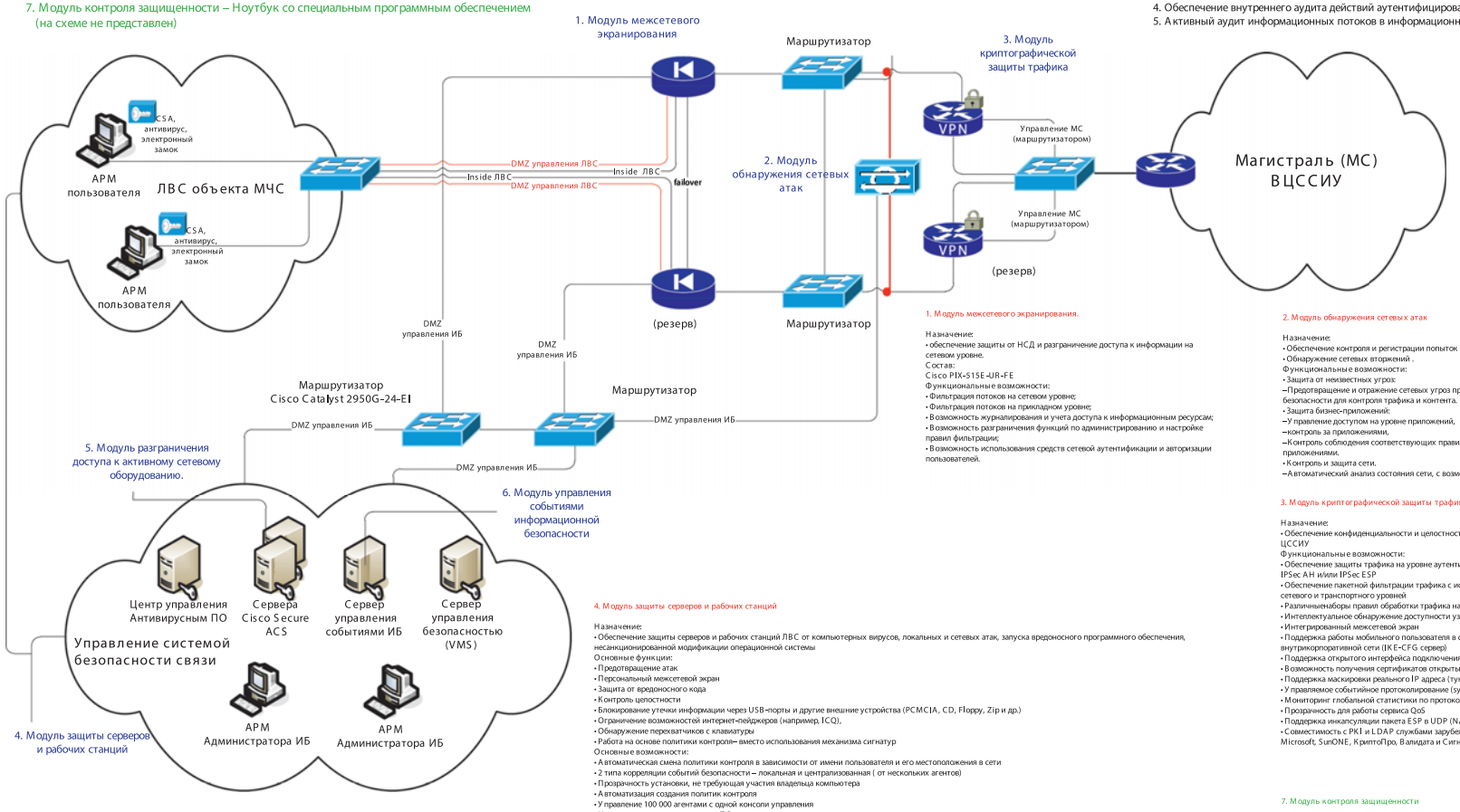

Рис. 1. Схема типового комплекса системы безопасности связи МЧС России

Назначение типового комплекса:

1. Защита информационных ресурсов МЧС России от внутренних и внешних угроз информационной безопасности;
2. Обеспечение целостности и доступности информации в условиях агрессивной информационной среды;
3. Минимизация последствий ущерба от разглашения, уничтожения, утечки и НСД к источникам информации ограниченного распространения;
4. Обеспечение внутреннего аудита действий аутентифицированных пользователей;
5. Активный аудит информационных потоков в информационном пространстве МЧС России.

1. Модуль межсетевого экранирования.

Назначение:
• обеспечение защиты от НСД и разграничение доступа к информации на сетевом уровне.
Состав:
Cisco PIX-515E-UR-FE
Функциональные возможности:
• Фильтрация потоков на сетевом уровне;
• Фильтрация потоков на прикладном уровне;
• Возможность журналирования и учета доступа к информационным ресурсам;
• Возможность разграничения функций по администрированию и настройке правил фильтрации;
• Возможность использования средств сетевой аутентификации и авторизации пользователей.

2. Модуль обнаружения сетевых атак

Назначение:
• Обеспечение контроля и регистрации попыток несанкционированного доступа;
• Обнаружение сетевых вторжений .
Функциональные возможности:
• Защита от неизвестных угроз:
–Предотвращение и отражение сетевых угроз при помощи комбинации из инновационных служб безопасности для контроля трафика и контента.
• Защита бизнес-приложений:
–Управление доступом на уровне приложений,
–контроль за приложениями,
–Контроль соблюдения соответствующих правил использования приложений, контроля за веб-приложениями.
• Контроль и защита сети.
–Автоматический анализ состояния сети, с возможностями активного управления и отражения угроз.

3. Модуль криптографической защиты трафика

Назначение:
• Обеспечение конфиденциальности и целостности информации, передаваемой по каналам связи ЦССИУ
Функциональные возможности:
• Обеспечение защиты трафика на уровне аутентификации/шифрации сетевых пакетов по протоколам IPSec AH и/или IPSec ESP
• Обеспечение пакетной фильтрации трафика с использованием информации в полях заголовков сетевого и транспортного уровней
• Различные наборы правил обработки трафика на различных интерфейсах
• Интеллектуальное обнаружение доступности узла сети (DPD)
• Интегрированный межсетевой экран
• Поддержка работы мобильного пользователя в соответствии с политикой безопасности внутрикорпоративной сети (IKE-CFG сервер)
• Поддержка открытого интерфейса подключения криптографических модулей
• Возможность получения сертификатов открытых ключей по протоколу LDAP
• Поддержка маскировки реального IP адреса (туннелирование трафика)
• Управляемое событийное протоколирование (syslog)
• Мониторинг глобальной статистики по протоколу SNMP, совместимость с CiscoWorks VPN Monitor
• Прозрачность для работы сервиса QoS
• Поддержка инкапсуляции пакета ESP в UDP (NAT traversal)
• Совместимость с PKI и LDAP службами зарубежных и российских производителей (RSA Keon, Microsoft, SunONE, КриптоПро, Валидата и Сигнал-КОМ)

4. Модуль защиты серверов и рабочих станций

Назначение:
• Обеспечение защиты серверов и рабочих станций ЛВС от компьютерных вирусов, локальных и сетевых атак, запуска вредоносного программного обеспечения, несанкционированной модификации операционной системы
Основные функции:
• Предотвращение атак
• Персональный межсетевой экран
• Защита от вредоносного кода
• Контроль целостности
• Блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD, Floppy, Zip и др.)
• Ограничение возможностей интернет-пейджеров (например, ICQ),
• Обнаружение перехватчиков с клавиатуры
• Работа на основе политики контроля– вместо использования механизма сигнатур
Основные возможности:
• Автоматическая смена политики контроля в зависимости от имени пользователя и его местоположения в сети
• 2 типа корреляции событий безопасности – локальная и централизованная (от нескольких агентов)
• Прозрачность установки, не требующая участия владельца компьютера
• Автоматизация создания политик контроля
• Управление 100 000 агентами с одной консоли управления
• Инвентаризация установленного ПО
• Интеграция с VPN-клиентами компаний Cisco и Check Point
• Интеграция с Network Admission Control (NAC)
• Делегирование отдельных функций управления агентом пользователю
• Механизм Trusted QoS
• Функционирование на платформах Windows, Linux, Solaris, VMWare
• Интеграция с сетевыми системами предотвращения атак
• Специальная группа правил для блокирования утечки информации

5. Модуль разграничения доступа к активному сетевому оборудованию

Назначение:
• Обеспечение аутентификации и разграничение доступа операторов и администраторов активного сетевого оборудования ЛВС.
Функциональные возможности:
• Поддержка Cisco NAC.
• Возможность масштабируемости.
• Создание профилей правил политик доступа к ресурсам.
• Использование расширенных компонентов репликации.
• Усиленная поддержка гибкой аутентификации по EAP с безопасным туннелированием (FAST) - EAP-FAST.
• Загружаемые списки IP ACL.
• Возможность сопоставления списков аннулированных сертификатов (CRL).
• Ограничение доступа АРМ.
• Использование фильтра сетевого доступа (NAF).

6. Модуль управления событиями ИБ

Назначение:
• обеспечивает сбор, корреляцию и анализ событий ИБ.
Функциональные возможности:
☒Определяет инциденты безопасности
☒Коррелирует данные от устройств
☒Возможность автоматического блокирования атак
☒Позволяет наглядно демонстрировать руководителям уровень безопасности и выдавать отчеты о нарушениях режима ИБ

7. Модуль контроля защищенности

Назначение:
• Обеспечение периодического контроля защищенности серверов, рабочих станций, активного сетевого оборудования ЛВС
Особенности сканирующего ядра:
• Полная идентификация сервисов на случайных портах
• Проверка на уязвимость серверов со сложной нестандартной конфигурацией, когда сервисы имеют произвольно выбранные порты
• Эвристический метод определения типов и имен серверов
• Обработка RPC-сервисов (Windows и *nix) с их полной идентификацией
• Обеспечивание возможности определения RPC-сервисов и поиска уязвимостей в них, а также определения детальной конфигурации компьютера в целом
• Проверка слабости парольной защиты
• Глубокий анализ контента WEB-сайтов
• Осуществление поиска и анализа директорий доступных для просмотра и записи

- защита накапливаемой информации, в том числе ПДн, от несанкционированного удаления, изменения, ознакомления и копирования;
- защита целостности и конфиденциальности информации при ее передаче между объектовыми комплексами АС МЧС России по каналам связи, в том числе:
  - криптографическая аутентификация взаимодействующих сторон;
  - подтверждение подлинности и целостности доставленной информации;
  - защита от повтора, задержки и удаления сообщений;
  - защита от отказа от факта отправления и приема сообщений;
- контроль целостности общего и специального программного обеспечения для его защиты от несанкционированного изменения;
- антивирусная защита программного и информационного обеспечения;
- защита серверного и коммуникационного оборудования от вредоносного программного обеспечения и сетевых атак, осуществляемых из внешних сетей;
- централизованное управление именами, идентификационными параметрами и криптографическими ключами в соответствии с установленным регламентом и требованиями эксплуатационных документов;
- комплексный подход к применению специализированных аппаратных, программных и аппаратно-программных средств и систем защиты, сертифицированных ФСТЭК;
- защита доступности вычислительных и коммуникационных ресурсов объектового комплекса АС МЧС России, в том числе:
  - реализация автоматизированных процедур обнаружения и противодействия атакам на телекоммуникационные ресурсы, защищаемую информацию и информационные ресурсы объектового комплекса АС МЧС России;
  - централизованное накопление и автоматизированная обработка сведений о существенных для безопасности информации событиях, возникающих на серверном и телекоммуникационном оборудовании объектового комплекса АС МЧС России;
  - проведение регламентного анализа защищенности компонентов программно-аппаратных средств, сетевых протоколов, баз данных, операционных систем и т. п.;
  - предотвращение потери информации за счет включения средств резервирования, копирования и восстановления работоспособности системы после сбоев.

Построение осуществляется по следующим направлениям:

- организационно-методическое обеспечение — комплекс организационных и методических мероприятий, которые регламентируют вопросы обработки информации ограниченного доступа, в том числе персональных данных, и являются необходимыми для соответствия требованиям законодательства Российской Федерации в области защиты информационных ресурсов, содержащих ПДн;
- техническое обеспечение — комплекс программных и программно-аппаратных средств защиты информации, обеспечивающий выполнение технических требований к системе защиты информации, в том числе ПДн.

В части организационно-методического обеспечения создание информационной системы ПДн включает в себя выполнение следующих мероприятий:

- обследование процессов обработки и обеспечения безопасности ПДн;
- анализ рисков и формирование требований по защите ПДн;
- разработка проектных решений информационной безопасности по защите ПДн;
- разработка комплекта организационно-распорядительной документации.

При выполнении данных мероприятий учитываются методические и нормативные документы регуляторов в области защиты ПДн — ФСТЭК России и ФСБ России:

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России документом от 14 февраля 2008 года);
- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утверждена заместителем директора ФСТЭК России 15 февраля 2008 года);
- методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены ФСБ России 21 февраля 2008 года №149/54-144);
- приказ ФСТЭК №21 от 18 февраля 2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК №17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- 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 (утверждены ФСБ России 21 февраля 2008 года №149/6/6-622).

Техническое обеспечение информационных систем, обеспечивающее безопасность персональных данных типового комплекса, создается в составе следующих подсистем:

- защиты от НСД (выполняющей функции: управления доступом, регистрации и учета, обеспечения целостности);
- защиты межсетевого взаимодействия;
- криптографической защиты (криптографическая защита каналов связи между удаленными объектами разных уровней);
- обнаружения вторжений;
- анализа защищенности;
- антивирусной защиты;
- контроля защищенности.

Технические решения, обеспечивающие безопасность персональных данных, выбираются в соответствии с требованиям ФСТЭК России и ФСБ России.

Анализ существующих на сегодняшний день способов защиты информации позволяет выделить два основных подхода:

- первый, наукообразный подход, заключается в освоении, а затем и применении на практике необходимых инструментариев измерения уровня информационной безопасности;
- второй, практический подход, основан на поиске разумной стоимости системы защиты информации.

Оптимальное решение, при котором можно чувствовать себя относительно уверенно,— стоимость системы информационной безопасности должна составлять примерно 10–20% от стоимости всей информационной системы. Это и есть та самая оценка на основе практического опыта (best practice), которой можно уверенно оперировать, если не производить детальные расчеты.

Подход в обосновании затрат на информационную безопасность предполагает расчет обоснованности затрат по каждому из запланированных мероприятий и определение эффективности всего комплекса процессов проекта системы защиты.

В качестве главного показателя берется измерение стоимости информации для организации. Под стоимостью информации можно понимать два различных параметра:

- затраты организации на создание либо приобретение информации;
- размер убытков, возникающих вследствие нарушения нормального протекания информационных процессов.

По результатам первичной классификации информационные системы персональных данных во многих случаях относятся к 1 или 2 классам, требующим существенных затрат. Понизить требования по защите персональных данных можно путем обезличивания информационной системы, организации выделенных автоматизированных рабочих мест[2]. Кроме этого возможны следующие варианты снижения издержек:

- заключение договорных отношений с компаниями, которые обладают опытом реализации проектов по защите информации;
- использование свободно распространяемых операционных систем с более высоким уровнем программной безопасности;
- применение современных средств усиленной аутентификации: например, смарт-карт, персональных жетонов, биометрики[3] и т. д.[4]

Рис. 2. Структура системы информационной безопасности персональных данных МЧС России

На практике и системы защиты информации МЧС Росси применяются с учетом ряда факторов: цена, сравнительный уровень предоставляемых функций, простота установки и управления, возможность интеграции в единую систему управления. Современные средства защиты информации позволяют экономить средства не только на сокращении перечня технических устройств, но и на количестве рабочего персонала. Компоненты современной системы информационной безопасности могут управляться с единой консоли. Это достигается интеграционными решениями.

С экономической точки зрения, система информационной безопасности строится не на закупке «железа», а, прежде всего, на продуманной политике применения комплекса мер (в т. ч. административных), способных снизить риски информационной безопасности до приемлемого «остаточного» уровня.

Создание системы информационной безопасности МЧС России позволит обеспечить защиту информационных ресурсов, в частности персональных данных, в информационных системах МЧС России, а также обрабатывать служебную информацию ограниченного распространения, в том числе согласно Табелю срочных донесений МЧС России.

2 Бажин К. А., Белькович В. А., Дубов В. П., Захаров А. А., Михайлов Ю. А. Техническая защита персональных данных. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Под ред. А. А. Захарова. Тюмень: Изд. ТюмГУ, 2011, 148–150 с.

3 Биометрическая система аутентификации пользователей BioLink IDenium –сертифицированная ФСТЭК России. http://fstec.ru/sistema-sertifikatsii-tzi.

4 Постановление Правительства РФ от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».