

Решения Cisco для защиты персональных данных

Проблема

Мы постоянно находимся под контролем различных государственных и муниципальных органов власти, коммерческих и правоохранительных структур. Паспортные столы и поликлиники, банки и пенсионные фонды, гостиницы и ЖЭКи, ГИБДД и избирательные комиссии, кадровые агентства и HR-подразделения работодателей... Все они собирают, группируют, анализируют, систематизируют, передают, получают персональные данные о нас. И не всегда они прилагают усилия для охраны этих сведений; зачастую теряя их или продавая мошенникам и нечистым на руку покупателям.

Защита персональных данных (ПДн) последние годы была и остается одной из острейших проблем в информационной сфере и взаимоотношениях государства, граждан и бизнеса. Постоянные утечки информации из государственных органов, банков, операторов связи и медицинских учреждений, продажа этих данных в Интернете или на компьютерных лотках; все это наносит ущерб и нарушает основные права на неприкосновенность частной жизни, дарованные каждому гражданину Конституцией РФ.

Обзор законодательства по персональным данным

Для защиты основных свобод и прав граждан разные государства Европы приняли различные нормативно-правовые акты. Не стала исключением и Россия, где с 3-го января 2007 года вступил в действие Федеральный Закон РФ от 27 июля 2006 года №152-ФЗ «О персональных данных». Он направлен на реализацию конституционных положений, закрепляющих право каждого на неприкосновенность частной жизни и свободу информации, а также международных обязательств Российской Федерации по ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных в соответствии с Федеральным Законом от 19 декабря 2005 года №160 «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

Законом предусматриваются общие унифицированные требования к сбору и обработке персональных данных физических лиц во всех сферах, где используются эти данные, принципы трансграничной передачи персональных данных, а также меры государственного контроля за деятельностью государственных органов, органов местного самоуправления, юридических и физических лиц, связанной с обработкой персональных данных.

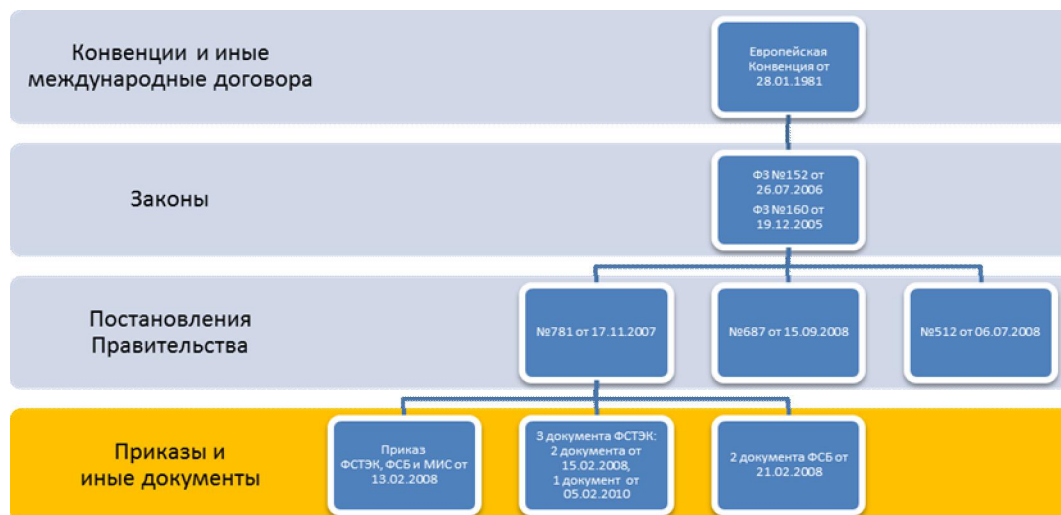


Рисунок 1. Структура основных нормативно-правовых актов в области защиты персональных данных

В соответствии со статьей 19 Федерального Закона «О персональных данных» Правительство Российской Федерации выпустило Постановление от 17 ноября 2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», которое определило общие требования по защите персональных данных, дальнейшая детализация которых была дана в нормативных правовых актах и методических документах Федеральной службы безопасности (ФСБ) и Федеральной службы по техническому и экспортному контролю (ФСТЭК):

- Приказ ФСТЭК, ФСБ и Мининформсвязи от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
- «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных», утвержденная ФСТЭК 14 февраля 2008 года.
- «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных», утвержденная ФСТЭК 14 февраля 2008 года.
- Приказ ФСТЭК от 5 февраля 2010 г. №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные ФСБ 21 февраля 2008 года.
- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащих сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в персональных системах персональных данных», утвержденные ФСТЭК 21 февраля 2008 года.

Неисполнение данных нормативных актов влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Таблица 1. Меры наказания за невыполнение требований законодательства по защите персональных данных

Статья	Нормативно-правовой акт	Название статьи	Максимальная мера наказания
5.27	КоАП	Нарушение законодательства о труде	50.000 руб. + приостановление деятельности на срок до 90 суток + дисквалификация должностного лица до 3-х лет
5.39	КоАП	Отказ в предоставлении или предоставлении неполной или ложной информации, затрагивающей гражданина	1.000 руб
13.11	КоАП	Нарушение порядка сбора, хранения, использования и распространения ПДн	10.000 руб

Таблица 1. Меры наказания за невыполнение требований законодательства по защите персональных данных (продолжение)

Статья	Нормативно-правовой акт	Название статьи	Максимальная мера наказания
13.12	КоАП	Нарушение правил защиты или использование несертифицированных средств защиты или нарушение условий лицензии ФСТЭК / ФСБ	20.000 руб. + конфискация + приостановление деятельности на срок до 90 суток
13.13	КоАП	Деятельность в области защиты ПДн без лицензии ФСТЭК / ФСБ	20.000 руб. + конфискация
13.14	КоАП	Разглашение персональных данных	5.000 руб.
19.4	КоАП	Невыполнение требований или воспрепятствование исполнению обязанностей ФСТЭК	10.000 руб.
19.5	КоАП	Невыполнение в срок требований надзорного органа или ФСТЭК	500.000 руб. + дисквалификация должностного лица до 3-х лет
19.6	КоАП	Непринятие мер по устранению нарушений	500 руб.
19.7	КоАП	Непредставление или представление в неполном или искаженном виде в Россвязькомнадзор сведений об операторе ПДн	5.000 руб.
19.20	КоАП	Осуществление деятельности без лицензии или с нарушением ее условий	20.000 руб. + приостановление деятельности на срок до 90 суток
137	УК	Нарушение неприкосновенности частной жизни	300.000 руб. + исправительные работы на срок до 240 часов + арест до 6-ти месяцев
171	УК	Незаконное предпринимательство	300.000 руб. + обязательные работы на срок до 1-го года + арест до 6-ти месяцев + лишение права занимать должность на срок до 5-ти лет
81	ТК	Разглашение охраняемой законом тайны	увольнение
90	ТК	Нарушение норм получения, обработки и защиты ПДн	увольнение
237	ТК	Неправомерные действия или бездействия работодателя	Размер возмещения морального ущерба определяет суд

Примечание: КОАП – Кодекс об административных правонарушениях РФ
 УК – Уголовный Кодекс РФ
 ТК – Трудовой Кодекс РФ.

Помимо исполнения указанных нормативных актов сегодня наметилась тенденция разработки и применения отраслевых стандартов и рекомендаций в области защиты персональных данных. На данный момент к их числу можно отнести:

- Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»
- Методические рекомендации для организации защиты информации при обработке ПДн в учреждениях здравоохранения, социальной сферы, труда и занятости, разработанные в Минздравсоцразвитии
- Требования Рособразования

- Стандарт Национальной ассоциации негосударственных пенсионных фондов «Организация обработки и защиты персональных данных в негосударственных пенсионных фондах»
- Стандарт Национальной ассоциации участников фондового рынка «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных операторами - профессиональными участниками рынка ценных бумаг»
- Рекомендации по защите персональных данных в информационных системах персональных данных оператора связи (НИР Тритон).

Детальные технические требования по защите персональных данных

Согласно перечисленным выше документам, выбор мероприятий и глубина их проработки по защите персональных данных зависит от типа и класса обрабатываемой их информационной системы. Полный список технических мер реализуется в виде соответствующих подсистем защиты персональных данных и выглядит следующим образом:

- антивирусная защита,
- межсетевое экранирование,
- обнаружение вторжений,
- обеспечение целостности,
- управление доступом,
- регистрация и учет,
- анализ защищенности,
- криптографическая защита,
- защита электронной почты,
- управление информационной безопасностью,
- защита от утечек по техническим каналам.

Реализация законодательства по персональным данным с помощью Cisco Secure Borderless Network

Решения Cisco в области защиты объединены в стратегию самозащищающейся сети Cisco Self-Defending Network, которая является частью концепции «Сети без границ» (Borderless Network). Ее идея достаточно проста: в настоящее время поддержание целостности и конфиденциальности корпоративной информации, включая и персональные данные, а также непрерывности бизнеса в течение всего жизненного цикла бизнес- и организационных процессов является ключом к успеху любой компании. Значение информации и контроля доступа к ней еще никогда не было так велико. Таким образом, задачей системы безопасности является предоставление своевременного доступа законным пользователям с одновременной возможностью обнаружения и предотвращения вторжений и иных нарушений безопасности на всех уровнях информационной системы. Современные сети должны реагировать на такие нарушения, сохраняя свою доступность, надежность и функциональность. Вместо того чтобы становиться жертвой, инфраструктура должна быть способна «поглощать» атаки и сохранять работоспособность, подобно иммунной системе человека, позволяющей организму функционировать при наличии в нем вирусов и бактериальных инфекций.

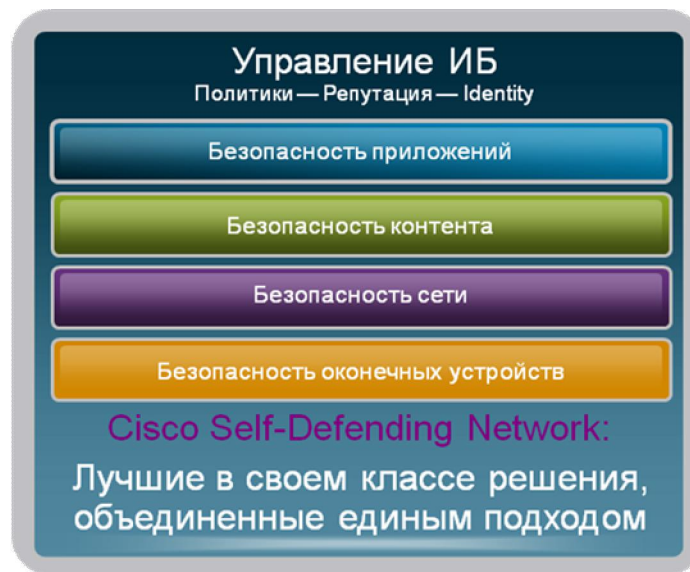


Рисунок 2. Стратегия самозащищающейся сети Cisco Self-Defending Network

Концепция самозащищающейся сети в рамках Cisco Borderless Network — это сквозная стратегия корпоративной или ведомственной обороны, поскольку она является основой для защиты всех данных, приложений и бизнес-процессов. Она представляет собой основную составляющую стратегии организаций по управлению рисками нарушения информационной безопасности, поскольку она предоставляет комплексный и системный подход к проблеме сетевой безопасности, поддерживающий общепризнанные в отрасли механизмы контроля и передовые методы безопасности, соответствующие требованиям российских регуляторов. Этот подход позволяет организациям защитить персональные данные, усовершенствовать механизмы управления операционными и информационными рисками и обеспечить их соответствие нормативным документам.

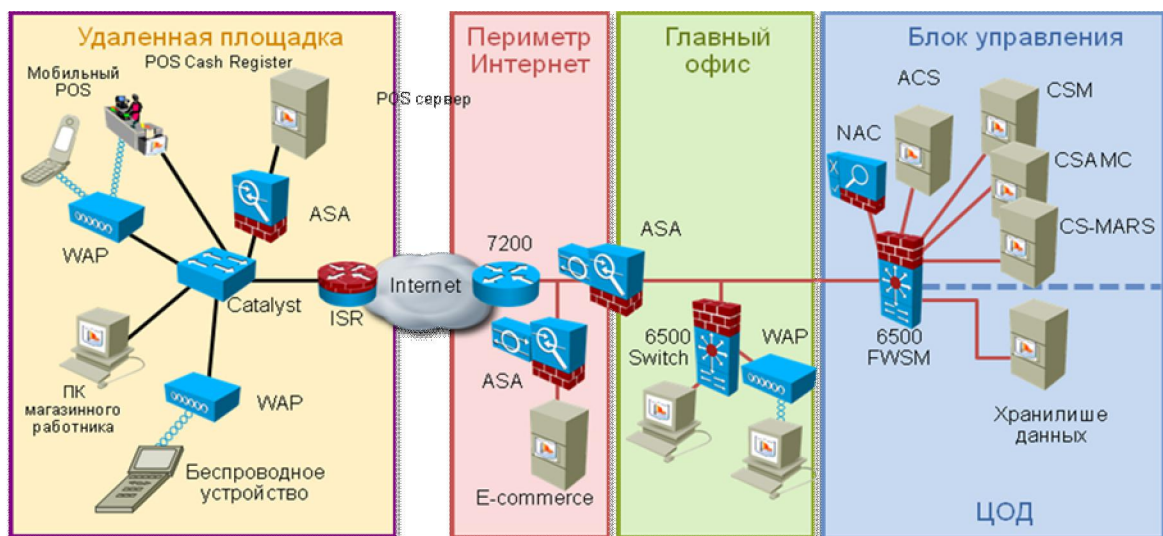


Рисунок 3. Архитектура Cisco для защиты персональных данных (представлены не все элементы)

Решения Cisco, входящие в Borderless Network, позволяют выполнить технические требования, которые указаны в вышеперечисленных нормативных документах, касающихся защиты персональных данных. Одним из ключевых требований, которые предъявляются к средствам защиты информации, применяемым в информационных системах, обрабатывающих персональные данные, является прохождение процедуры

оценки соответствия, включая сертификацию по требованиям безопасности информации. На сегодняшний день решения компании Cisco имеют свыше 500 сертификатов по требованиям информационной безопасности, выданных в России, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на отечественном рынке информационной безопасности.

Для криптографической защиты персональных данных компания Cisco предлагает разработанные совместно с российским производителем средств защиты, компанией С-terra СиЭсПи, VPN-решения – NME-RVPN для маршрутизаторов Cisco ISR и ISR G2, а также S-Terra VPN Gate на базе серверов Cisco UCS. Оба изделия сертифицированы в ФСБ по классу КС2.

Таблица 2. Продукты Cisco по ИБ, реализующие требования законодательства по персональным данным

Требования	ASA	IPS	ISR	RVPN	Catalyst	NAC	IronPort	ACS
Управление доступом	+		+		+	+		+
Обеспечение целостности	+		+			+		
Регистрация и учет	+	+	+	+	+	+	+	+
Межсетевое экранирование	+		+		+			
Обнаружение вторжений		+	+		+		+	
Антивирусная защита	+	+	+			+	+	
Анализ защищенности						+		
Защита электронной почты							+	
Криптографическая защита				+				

Примечание:

ASA — многофункциональные защитные устройства Cisco ASA 5500, а также модуль CSC-SSM,
 IPS — Cisco IPS 4200, Cisco IOS IPS, Cisco IPS-AIM, Cisco AIP-IPS,
 ISR — маршрутизаторы Cisco Integrated Services Router с функциями защиты,
 RVPN — криптографический модуль Cisco NME-RVPN Module для маршрутизаторов Cisco ISR,
 Catalyst — коммутаторы Cisco Catalyst и сервисные модули для Cisco Catalyst 6500 (IDSM, FWSM, ACE и т.д.),
 NAC — система контроля доступа Cisco NAC Appliance,
 IronPort — системы защиты электронной почты и Web-трафика IronPort E-mail Security Appliance и Web Security Appliance,
 ACS — система аутентификации, авторизации, регистрации и учета Cisco Secure Access Control Server.

Для управления решениями, указанными в таблице 2, используются системы Cisco Security Manager, а для проверки качества и эффективности их настройки — Cisco Network Compliance Manager.

Участие Cisco в разработке нормативных требований по защите ПДн

Помимо предложения эффективных технических решений по защите персональных данных, компания Cisco активно участвует и в нормотворческой деятельности по данному вопросу. В частности сотрудники российского офиса Cisco:

- Участвуют в экспертизе и выработке предложений по изменению законопроектов в области персональных данных.
- Входят в оргкомитет Общественных слушаний по совершенствованию законодательства в области персональных данных.
- Входят в Консультационный центр Ассоциации Российских Банков (АРБ) по вопросам применения отдельных норм Федерального закона №152-ФЗ «О персональных данных».

- Участвовали в работе рабочей группы Банка России и АРБ по разработке 4-й версии Комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» в части требований по защите персональных данных.
- Участвуют в экспертизе отраслевых стандартов и требований федеральных органов исполнительной власти по защите персональных данных.

Заключение

Безопасность персональных данных – одна из приоритетных задач на сегодняшний день. Ее важность определяется не только наличием 15-ти статей в Уголовном и Трудовом Кодексах, а также Кодексе об административных правонарушениях, и предусматривающих наказание за нарушение законодательства по персональным данным, но и вхождением России в мировое сообщество, уже давно прилагающее немало усилий к защите основных свобод и прав граждан, к числу которых относится и тайна частной жизни. Активизация деятельности России на мировой арене, активное сотрудничество с Евросоюзом, вступление в ВТО, требования ОЭСР и ООН... Все это заставляет нас уделять больше внимания защите персональных данных граждан, своих сотрудников, заказчиков, партнеров, контрагентов. И компания Cisco, обладающая многолетним опытом работы в области информационной безопасности, а также принимающая активное участие в разработке и экспертизе нормативных требований по защите персональных данных, готова помочь в решении данной задачи.



Cisco
Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., 52, стр. 1, 4-й этаж.
Телефон: +7 (495) 961 1410
Факс: +7 (495) 961 1469
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186, Санкт-Петербург,
бизнес-центр «Регус»,
Невский пр-т, 25, 2-й этаж, офисы 9, 30.
Телефон: +7 (812) 336 6531
Факс: +7 (812) 346 7800
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск,
бизнес-центр «Росэнергогаз»,
Димитрова пр-т, 2, 5-й этаж.
Телефон: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Arionet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanel, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)