Техническая защита персональных данных

Что необходимо знать специалистам по ИТ и кибербезопасности в области технической защиты персональных данных

Краткие выводы

Чтобы не тратить время наших заказчиков на чтение большого количества объемных нормативных правовых актов по технической защите персональных данных, компания Cisco подготовила краткое руководство по ним, которое тезисно можно описать следующим образом:

1. Российское законодательство по технической защите персональных данных должна соблюдать любая организация, работающая на территории России, независимо от формы ее собственности, сферы экономики и размера. Законодательство называет такую организацию оператором персональных данных.
2. Российские организации также могут быть обязаны выполнять требования европейского законодательства по защите персональных данных (GDPR), которое в технической части не противоречит российским требованиям.
3. Регуляторами по технической защите персональных данных являются ФСТЭК России (все вопросы кроме криптографии) и ФСБ России (только криптографическая защита персональных данных). Некоторые вопросы также регулирует Банк России (для финансовых организаций).
4. Меры безопасности оператор персональных данных определяет самостоятельно.
5. Техническая защита персональных данных может быть реализована своими силами или с помощью компании, обладающей лицензией ФСТЭК на деятельность по технической защите конфиденциальной информации.
6. Меры по безопасности персональных данных зависят от актуальных угроз, которые оператор персональных данных определяет самостоятельно или, в отдельных случаях, опираясь на нормативные акты федеральных органов исполнительной власти или Банка России.
7. Общие требования по технической защите персональных данных установлены в приказе ФСТЭК №21 и, в случае применения шифровальных средств, в приказе №378 ФСБ России. Эти требования не противоречат международным стандартам и сводам лучших практик – ISO 27701, CNIL, Cyber Essentials, ISO 29000, ENISA и т.п.
8. Минимально необходимый набор защитных мер в явной форме отсутствует, но есть базовый или рекомендуемый набор в 21-м приказе ФСТЭК России. Этот набор может быть расширен или сужен в зависимости от актуальных угроз и используемых информационных технологий.
9. Применение сертифицированных средств шифрования для защиты персональных данных является необязательным.
10. Оценка соответствия средств защиты персональных данных обязательна, но необязательно в виде сертификации ФСТЭК России или ФСБ России.
11. Невыполнение требований российского законодательства влечет за собой преимущественно административную ответственность, но в области технической защиты персональных данных правоприменительная практика незначительна. Существуют также серьезные штрафы за нарушение европейских требований по защите персональных данных (GDPR), которые могут быть наложены в ЕС.
12. Cisco обладает необходимым портфолио программных, программно-аппаратных, виртуальных и облачных решений по безопасности персональных данных.

ПРЕДУПРЕЖДЕНИЕ

- Приведенные в настоящем документе мнения и рекомендации не являются юридическим заключением или позицией регулирующих органов власти и не могут заменять собой необходимость получения юридической консультации в конкретных практических ситуациях и в конкретных юрисдикциях, целесообразность обращения за которыми следует рассматривать при решении конкретных практических задач.

Нормативные правовые акты

Федеральный закон №152

Федеральный закон от 27.06.2006 «О персональных данных» регулирует отношения, возникающие при обработке персональных данных действующих, бывших и потенциальных сотрудников и клиентов, а также иных лиц, чьи персональные данные обрабатываются в организации.

Безопасность персональных данных при их обработке в информационной системе, согласно статье 19 Федерального закона, обеспечивается с помощью системы защиты персональных данных, которая должна нейтрализовать актуальные угрозы, определяемые согласно Постановлению Правительства №1119. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора, т.н. обработчиком.

Выбор мер защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России), а именно приказом №378 и приказом №21 соответственно.

Постановление Правительства №1119

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливает высокоуровневые, преимущественно организационные, требования к защите персональных данных, а также правила определения уровней защищенности таких данных, от которых зависит набор защитных мер, определенных Постановлением Правительства и приказами ФСТЭК России и ФСБ России соответственно.

Решение о выборе типа актуальных угроз безопасности персональных данных, актуальных для информационной системы, принимается оператором персональных данных самостоятельно, если для них не разработано нормативных правовых актов, определяющих актуальные угрозы безопасности (так сделано Банком России для финансовых организаций). При этом, под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих **актуальную**, а не теоретическую опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Для абсолютного большинства операторов персональных данных, по нашему мнению, актуальными являются угрозы только 3-го, минимального, типа.

Указания Банка России №3889-У и 4859-У

Указание Банка России от 10.12.2015 №3889-У "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных" определяет угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных кредитных организаций и некредитных финансовых организаций. Данное указание не определяет угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, относящихся к биометрическим персональным данным, персональным данным, полученным из общедоступных источников. Модель угроз для биометрических персональных данных определена в Указании Банка России №4859-У, Публичного акционерного общества "Ростелеком" №01/01/782-18 от 09.07.2018 "О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", в единой биометрической системе". .

ПРЕДУПРЕЖДЕНИЕ

- Приведенные в настоящем документе мнения и рекомендации не являются юридическим заключением или позицией регулирующих органов власти и не могут заменять собой необходимость получения юридической консультации в конкретных практических ситуациях и в конкретных юрисдикциях, целесообразность обращения за которыми следует рассматривать при решении конкретных практических задач.

Приказ ФСТЭК №21

Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» определяет меры по обеспечению безопасности персональных данных для каждого из уровней защищенности персональных данных, установленных в Постановлении Правительства №1119. Список из более чем 150 возможных мер приведен в приложении к приказу и представляет собой каталог, из которого оператор персональных данных выбирает защитные меры, соответствующие актуальным угрозам и особенностям технологии обработки персональных данных и используемым для этого информационным технологиям.

Приказ ФСБ №378

Согласно Федеральному закону «О персональных данных» оператор персональных данных обязан обеспечивать их конфиденциальность, которая может быть реализована различными способами, в том числе и путем применения средств криптографической защиты информации. В этом случае должен применяться Приказ ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», устанавливающий требования к средствам криптографической защиты и особенностям их эксплуатации. Средства криптографической защиты информации в этом случае должны иметь сертификат ФСБ России.

ГОСТ 57580.1

Финансовые организации, кредитные и некредитные, при обеспечении безопасности информации, включая и персональные данные, дополнительно к приказам №21 и №378 должны руководствоваться "ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", который определяет соответствие уровней защищенности персональных данных и уровней защиты информации, установленных ГОСТом, а также состав и содержание организационных мер, связанных с обработкой финансовой организацией персональных данных.

Директива Евросоюза (GDPR)

Организации, которые обрабатывают персональные данные граждан Евросоюза, помимо указанных выше нормативных правовых актов обязаны соблюдать требования Общего регламента защиты персональных данных, известного как GDPR (General Data Protection Regulation). Данный нормативный правовый акт не устанавливает перечня обязательных защитных, как не устанавливает и требований к применяемым средства защиты персональных данных, допуская использование в качестве сборника лучших практик по защите персональных данных существующие стандарты – CNIL, ISO 27701, ISO 27018, ISO 29151, ENISA и даже приказ ФСТЭК №21.

Ответы на часто задаваемые вопросы

Какой стандарт или фреймворк лучше использовать для защиты персональных данных?

Идеального стандарта или фреймворка для построения системы защиты персональных данных не существует – выбор зависит от опыта работы с имеющимися стандартами, отрасли, в которой работает оператор персональных данных, обязательных требований, установленных законодательством, а также необходимости защищать иные виды информации ограниченного доступа. По опыту Cisco вполне возможно использование в качестве основы для построения системы защиты персональных данных стандарта ISO 27701, серии стандартов ISO 29000, свода лучших практик NIST Cybersecurity Framework или набора стандартов Банка России с выбором защитных мер, согласно требованиям ФСТЭК России и ФСБ России.

Есть ли обязательные меры защиты персональных данных?

В настоящий момент времени отсутствует обязательный или минимально необходимый перечень защитных мер, которые должны быть применены для защиты персональных данных. Перечень таких мер определяется оператором персональных данных самостоятельно, базируясь на требованиях нормативных правовых актов ФСТЭК России, ФСБ России, Банка России, в пределах их полномочий.

ПРЕДУПРЕЖДЕНИЕ

- Приведенные в настоящем документе мнения и рекомендации не являются юридическим заключением или позицией регулирующих органов власти и не могут заменять собой необходимость получения юридической консультации в конкретных практических ситуациях и в конкретных юрисдикциях, целесообразность обращения за которыми следует рассматривать при решении конкретных практических задач.

Какие меры защиты персональных данных надо применять?

В состав мер, установленных ФСТЭК России, и обеспечивающих безопасность персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Как выбираются меры защиты персональных данных?

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, осуществляется оператором персональных данных самостоятельно и включает в себя:

- определение базового (рекомендуемого) набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных
- адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе)
- уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер
- дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации (например, требований Банка России для финансовых организаций).

Иными словами, можно ориентироваться на базовый набор и применять защитные меры, указанные в приложении к Приказу ФСТЭК №21 применительно к конкретному уровню защищенности, а можно, отталкиваясь от базового набора, путем его расширения и сокращения разработать собственный набор защитных мер, лучше всего подходящих для конкретной информационной системы персональных данных.

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

ПРЕДУПРЕЖДЕНИЕ

- Приведенные в настоящем документе мнения и рекомендации не являются юридическим заключением или позицией регулирующих органов власти и не могут заменять собой необходимость получения юридической консультации в конкретных практических ситуациях и в конкретных юрисдикциях, целесообразность обращения за которыми следует рассматривать при решении конкретных практических задач.

Можно ли применять несертифицированные средства защиты информации?

В соответствии с законодательством Российской Федерации о персональных данных в информационных системах персональных данных для защиты персональных данных необходимо применять средства защиты информации, прошедшие процедуру оценки соответствия **в любой** из предусмотренных законодательством о техническом регулировании форм. Только для обеспечения безопасности персональных данных, обрабатываемых в государственных информационных системах, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации. Это означает, что для информационных систем персональных данных, не имеющих статуса государственных, обязательная сертификация средств защиты по требованиям безопасности является **необязательной**.

Согласно законодательству о техническом регулировании, существует множество форм оценки соответствия, среди которых можно назвать ввод в эксплуатацию, испытания, декларирование соответствия, государственный контроль и надзор, добровольная сертификация и т.п. В случае отсутствия явного указания, установленного Указом Президента, Федеральным законом или Постановлением Правительства, на форму оценки соответствия, ее форму оператор персональных данных выбирает самостоятельно.

В том случае, если оператор персональных данных принимает решение о применении средств защиты информации, прошедших процедуру оценки соответствия в форме обязательной сертификации, то должны применяться средства защиты информации, соответствующие требованиям Приказа ФСТЭК №21.

Обязательно ли использовать шифровальных средства для защиты персональных данных?

Требование по обязательному применению средств криптографической защиты информации (шифровальных средств) для защиты персональных данных федеральным законом не предусмотрено.

Как можно обеспечить конфиденциальность персональных данных?

Выбор конкретного метода обеспечения конфиденциальности персональных данных зависит от актуальных угроз (поэтому так важно иметь качественную модель угроз) для них и используемых информационных технологий обработки персональных данных. Среди таких методов можно назвать:

- использование технологии виртуальных сетей на основе меток безопасности (VLAN, TrustSec или MPLS)
- архивирование персональных данных
- обработка персональных данных в рамках контролируемой зоны
- использование оптических каналов связи
- перевести персональные данные в разряд общедоступных или получить согласие субъекта на их передачу в открытом виде
- реализовать принцип минимума привилегий и ограничить круг лиц, имеющих доступ к персональным данным
- обезличить персональные данные
- правильное определение границ информационной системы персональных данных
- использовать средства криптографической защиты информации.

Как защитить <технологию>/<сервис>, использующую персональные данные?

Ввиду отсутствия требований и рекомендаций, определяющих меры защиты информационных систем персональных данных (исключая отдельные случаи подключения к государственным информационным системам), разработанных органами законодательной и исполнительной власти, оператор персональных данных может ориентироваться на иные разработанные документы и своды лучших практик, в том числе:

- «Защита персональных данных в онлайн-сервисах (https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf)
- «Использование персональных данных в облачных вычислениях» (https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf)

ПРЕДУПРЕЖДЕНИЕ

- Приведенные в настоящем документе мнения и рекомендации не являются юридическим заключением или позицией регулирующих органов власти и не могут заменять собой необходимость получения юридической консультации в конкретных практических ситуациях и в конкретных юрисдикциях, целесообразность обращения за которыми следует рассматривать при решении конкретных практических задач.

- «Использование персональных данных в рамках концепции Bring Your Own Device» (https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf)
- «Руководство по безопасности обработки персональных данных» (https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing)
- «Защита персональных данных в мобильных приложениях» (https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications)
- «Защита персональных данных в облачных средах» (https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds)
- «Безопасность персональных данных в блокчейне и распределенных реестрах» (https://www.iso.org/standard/75061.html)
- «Защита персональных данных при использовании Больших данных, искусственного интеллекта и машинного обучения» (https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf)
- «Защита персональных данных в технологии Больших данных» (https://www.enisa.europa.eu/publications/big-data-protection)
- «Обработка персональных данных и искусственный интеллект» (https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf).

Какие средства защиты персональных данных мне использовать?

За исключением ситуации с защитой персональных данных в государственных информационных системах, существующие нормативные правовые акты не ограничивают оператора персональных данных в выборе средств защиты персональных данных. Главное, чтобы указанные средства защиты нейтрализовали актуальные угрозы персональным данным, определенные их оператором.

Как мне убедиться, что у меня с защитой все хорошо?

Оценка эффективности реализованных защитных мер проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

Какие регуляторы могут осуществлять контроль и надзор за технической защитой персональных данных?

В соответствие с Федеральным законом «О персональных данных» контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в государственных информационных системах персональных данных осуществляются ФСТЭК России и ФСБ России в пределах их полномочий. В иных информационных системах персональных данных, эксплуатируемых негосударственными организациями, контроль и надзор может быть осуществлен ФСТЭК России и ФСБ России только по отдельному решению Правительства.

Что будет за нарушение требований по защите персональных данных?

За нарушение требований по защите персональных данных предусмотрена административная ответственность согласно статье 13.12 Кодекса об административных правонарушениях, а именно:

- Использование несертифицированных средств защиты информации, если они подлежат обязательной сертификации – штраф на юридическое лицо **до 25 тысяч рублей**.
- Нарушение требований о защите информации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации – штраф на юридическое лицо **до 15 тысяч рублей**.

Решения и сервисы Cisco

Cisco обладает не только специализированными сервисами, позволяющими выполнить требования, например, GDPR, по защите персональных данных, но и широким портфолио, которое позволяет выполнить технические меры защиты, указанные в вышеперечисленных нормативных правовых актах, включая ФСТЭК России, ФСБ России, Банк России, GDPR и другие. Все эти решения могут пройти оценку соответствия в любой из предусмотренных законодательством о техническом регулировании форм, а часть из них также имеет сертификаты ФСТЭК России, например, межсетевые экраны Cisco Firepower, средство контроля доступа Cisco ISE, системы предотвращения вторжений Cisco NGIPS и т.п.

ПРЕДУПРЕЖДЕНИЕ

- Приведенные в настоящем документе мнения и рекомендации не являются юридическим заключением или позицией регулирующих органов власти и не могут заменять собой необходимость получения юридической консультации в конкретных практических ситуациях и в конкретных юрисдикциях, целесообразность обращения за которыми следует рассматривать при решении конкретных практических задач.

Требования	ASA / ASAv	Firepower	NGIPS / wIPS	AMP4E	ISE / TrustSec	ESA	WSA / Umbrella	SWE / SWC	AC	Tetration
Идентификация и аутентификация	+	+	+		+	+	+		+	
Управление доступом	+	+	+	+	+	+	+	+	+	
Ограничение программной среды										
Защита машинных носителей ПДн					+					
Регистрация событий безопасности	+	+	+	+	+	+	+	+	+	+
Антивирусная защита				+						
Обнаружение вторжений		+	+	+			+	+		
Анализ защищенности		+			+			+		
Обеспечение целостности		+	+	+		+	+			
Обеспечение доступности	Обеспечивается любым решением компании Cisco, в т.ч. и не относящимся к решениям по информационной безопасности									
Защита среды виртуализации		+	+	+	+			+		+
Защита технических средств										
Защита информационной системы	+	+	+	+	+	+	+	+	+	
Управление инцидентами		+	+	+	+			+		
Управление конфигурацией	Обеспечивается системами управления сетью и информационной безопасности									

Примечание

- ASA – Cisco ASA 5500-X (5512, 5515, 5525, 5545, 5555, 5585), Cisco Firepower с ПО ASA, а также IOS Firewall
- Firepower – Firepower 1000, 2100, 4100, 9300 с ПО Firepower Threat Defense
- NGIPS – Cisco Firepower NGIPS
- wIPS – Cisco Wireless Adaptive IPS
- AMP4E – Advanced Malware Protection for Endpoint
- ISE – Cisco Identity Service Engine, включая Virtual ISE
- ESA – Cisco E-mail Security Appliance, включая Virtual ESA
- WSA – Cisco Web Security Appliance, включая Virtual WSA
- SWE – Cisco Stealthwatch Enterprise
- SWC – Cisco Stealthwatch Cloud
- AC – Cisco AnyConnect

Дополнительная информация

- Подходы Cisco к реализации требований GDPR и защите персональных данных в собственных решениях – https://www.cisco.com/c/en/us/about/trust-center/gdpr.html
- Решения Cisco по реализации требований GDPR – https://www.cisco.com/c/en/us/products/security/general-data-protection-regulation.html
- Решения Cisco по защите персональных данных – https://www.cisco.com/c/en/us/products/security/privacy-data-protection-cybersecurity.html
- Сервис Cisco по реализации требований GDPR – https://www.cisco.com/c/dam/en/us/services/collateral/se/security-gdpr-aag.pdf
- Блог Cisco о GDPR – https://blogs.cisco.com/tag/gdpr
- https://www.cisco.com/c/dam/en/us/products/collateral/security/data-protection-services.pdf
- Отчет Cisco “From Privacy to Profit” – https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf