КапиталЪ
Управляющая компания

Защита персональных данных – ждать или действовать ?

По каким правилам играем сейчас?

- **Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;**
- **Постановление Правительства РФ от 17.11.07 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;**
- **Приказ ФСТЭК от 05.02.10 №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».**

По каким правилам играем сейчас?

Приказ ФСТЭК №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»

В основу Приказа положен следующий документ:

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 года

По каким правилам играем сейчас?

Требования к АС первой группы

Обозначения:

" - " - нет требований к данному классу;

" + " - есть требования к данному классу.

Подсистемы и требования	**Классы**				
	1Д	**1Г**	**1В**	**1Б**	**1А**
Использование сертифицированных средств защиты	-	-	+	+	+

При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться на классы защищенности АС не ниже 3А, 2А, 1А, 1Б, 1В

Что можно ждать в будущем?

- **Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" СТО БР ИББС-1.0-2010"**

  (принят и введен в действие Распоряжением Банка России от 21.06.2010 N Р-705)

- **Предложения государственных органов по гармонизации законодательства**

- **Законопроект №282499-5 Депутата ГД В.М.Резника**

  О внесении изменений в Федеральный закон "О персональных данных"(в части уточнения условий и правил обработки персональных данных)

Что можно ждать в будущем?

- **Стандарт Банка России СТО БР ИББС-1.0-2010**

  Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС) введен в действие 21 июня 2010 года. Документы согласованы ФСБ , Роскомнадзором, ФСТЭК 28 июня 2010.

- **Отсутствие необходимости получать лицензию на ТЗКИ**

  В настоящем стандарте требование получения лицензии на деятельность по технической защите конфиденциальной информации (информации ограниченного доступа) при проведении мероприятий по обеспечению безопасности в специальных ИСПДн для собственных нужд организаций БС РФ, а также требование проведения аттестации специальных ИСПДн не устанавливаются. В случае введения в действие стандарта в организации БС РФ указанные требования не являются обязательными при проведении комплекса мероприятий по обеспечению безопасности персональных данных в специальных ИСПДн организаций БС РФ.

- **Отсутствие необходимости использовать сертифицированные СЗИ**

  В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД.

- **Основные информационные системы банков, в которых и содержится подавляющая часть ПДн можно вообще не причислять к ИСПДн !**

  В организации БС РФ должен быть определен и документально зафиксирован подход к отнесению АБС к информационным системам персональных данных (ИСПДн).В организации БС РФ должен быть определен и документально зафиксирован перечень ИСПДн. В перечень ИСПДн должны быть включены как минимум АБС, целью создания и использования которых является обработка персональных данных.АБС, реализующие банковские платежные технологические процессы, не относятся к ИСПДн.

Большая часть кредитных организаций России приняли стандарт либо планируют это сделать. Общая доля кредитных организаций, принявших стандарт, ожидается на уровне 75-80%.

Что можно ждать в будущем?

- **Предложения государственных органов по гармонизации законодательства:**

- Внести изменения в части ужесточения ответственности операторов за несоблюдение организационных и технических мер, повлекших за собой нарушение прав и законных интересов субъектов персональных данных **(Роскомнадзор)**
- Предоставить исключительно Банку России права устанавливать для банковской системы Российской Федерации стандарты и требования по обеспечению безопасности информации (для персональных данных - по согласованию с регуляторами) **(АРБ)**
- Включить требование соразмерности мер по обеспечению безопасности персональных данных возможному размеру ущерба субъекту персональных данных и возможности возникновения такого ущерба **(Центробанк)**

Что можно ждать в будущем?

- **Предложения Комитета по безопасности Государственной Думы**

- Обязательные требования целесообразно отнести к операторам информационных систем, содержащих персональные данные, создаваемых в соответствии с законодательством Российской Федерации. Остальные операторы обязаны защищать создаваемые системы либо в рамках режимов конфиденциальности, распространяемых на информационную систему в целом (в частности, режимы защиты государственной тайны, банковской тайны, налоговой тайны и иных видов тайн, установленных федеральным законом), либо исходя из общих стандартов защиты информации (например, Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных Приказом Гостехкомиссии России от 30.08.2002 № 282), самостоятельно определяя адекватные методы и средства защиты персональных данных с учетом их природы, объема обрабатываемых данных, стоимости применения мер защиты, характеристик информационных систем оператора и учитывая рекомендации регулирующих органов.
- Внести изменения в ст. 17 Федерального закона «О лицензировании отдельных видов деятельности» и Постановления Правительства от 15 августа 2006 г. N 504 «О лицензировании деятельности по технической защите конфиденциальной информации» в части ограничения сферы лицензирования деятельности по технической защите информации («за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя»).
- Уточнить требования по использованию исключительно сертифицированных средств защиты информации, которые являются практически невыполнимыми, поскольку в связи с динамичным развитием информационных технологий оценка соответствия каждой версии программного обеспечения занимает существенно дольше времени, чем жизненный цикл этой версии.

Что можно ждать в будущем?

- **Законопроект №282499-5 Депутата ГД В.М.Резника**
  О внесении изменений в Федеральный закон "О персональных данных"(в части уточнения условий и правил обработки персональных данных) :

- Соглашение предполагает урегулирование следующих аспектов обработки персональных данных: … перечень и характер мер, принимаемых оператором для обеспечения безопасности обрабатываемых персональных данных.

- Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. В случаях, установленных федеральными законами, определяющими случаи обязательной обработки персональных данных и (или) особенности обработки персональных данных, Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в государственных и муниципальных информационных системах персональных данных.

- При обработке персональных данных на основе согласия перечень мер по обеспечению безопасности персональных данных при их обработке определяется соглашением оператора и субъекта персональных данных.

Что делать сейчас ?

- **План по приведению деятельности Организации в соответствие с требованиями Федерального закона «О персональных данных» согласно отраслевым стандартам**

- Изучить бизнес-процессы Организации и технологические процессы обработки информации.
- Идентифицировать и описать все бизнес-процессы (технологические процессы), в рамках которых обрабатываются персональные данные
- Определить какие программные и технические средства используются в технологических процессах, в рамках которых обрабатываются персональные данные.
- Определить работников Организации (наименование должностей), участвующих в технологических процессах, в рамках которых обрабатываются персональные данные.
- Определить состав обрабатываемых в Организации персональных данных (тип, категория, объем).
- Определить цели, правовое основание, условия и принципы обработки персональных данных.
- Определить, выполняется ли обработка специальных категорий и/или биометрических персональных данных. Если да, то определить, на каком основании выполняется обработка таких персональных данных.
- Сопоставить объем собираемых персональных данных целям обработки (исключить избыточные данные).
- Определить срок хранения персональных данных.
- Определить порядок получения согласия на обработку персональных данных для тех случаев, когда необходимо получить такое согласие в письменном виде.
- Определить персональные данные, получаемые не от субъекта персональных данных и порядок предоставления в данных случаях субъекту персональных данных предусмотренной законодательством Российской Федерации информации
- Определить порядок передачи персональных данных сторонним организациям и лицам.
- Определить договорные взаимоотношения, в рамках которых выполняется передача персональных данных третьей стороне, и внести в такие договора требования об обеспечении конфиденциальности передаваемых персональных данных.
- Определить, выполняется ли трансграничная передача персональных данных.
- Определить порядок реагирования на запросы со стороны субъектов персональных данных и предоставления им их персональных данных, внесения изменений, прекращения обработки персональных данных.
- Определить порядок уничтожения персональных данных после достижения целей обработки.

Что делать сейчас ?

- Определить структурное подразделение или должностное лицо (лиц), ответственное (ых) за обеспечение безопасности персональных данных в Организации.
- Провести анализ информационных систем Организации и составить перечень систем, в которых обрабатываются персональные данные. Выделить ИСПДн.
- Выявить ИСПДн (в том числе государственные) и их границы (в рамках Организации), в отношении которых Организация не определяет цели обработки и требования по защите (например, передача отчетности в Пенсионный фонд, ФНС, ФОМС и др.)
- Разработать Частную модель угроз безопасности персональных данных при их обработке в ИСПДн.
- Провести классификацию ИСПДн.
- Оценить необходимость и возможности обезличивания персональных данных. Провести обезличивание персональных данных. При необходимости провести повторную классификацию ИСПДн.
- Разработать требования по обеспечению безопасности персональных данных при обработке в ИСПДн.
- Разработать должностные инструкции персонала ИСПДн в части обеспечения безопасности персональных данных при их обработке в ИСПДн.
- Провести анализ существующих защитных мер на предмет соответствия требованиям нормативных правовых актов.
- Провести выявление невыполненных в Организации требований нормативных правовых актов, провести принятие решений о создании системы защиты персональных данных, о доработке ИСПДн, о доработке документов Организации и др.
- Разработать технические задания на создание системы защиты персональных данных. Разработать частные технические задания на доработку ИСПДн. Или описать имеющиеся ИСПДн и СЗПДн.
- Вести учет носителей персональных данных, СЗИ.
- Обеспечить размещение специального оборудования, охрану и организацию режима в помещениях.
- Определить подразделения и назначить лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности персональных данных.
- Провести обучение лиц, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними.
- Доработать существующие документы и разработать новые документы с целью приведения документов Организации в соответствие с требованиями Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ и иных нормативных правовых актов
- Провести оценку соответствия обеспечения безопасности персональных данных требованиям нормативных правовых актов.

Помогут ли отсрочки ?

- **Какие изменения принесла отсрочка 2010 года ?**

В опубликованных документах ФСТЭК (по сравнению с первоначальными версиями ДСП) отменены требования:

- **Обязательной аттестации ИСПДн;**
- **Обязательного получения лицензии на ТЗКИ**

  На необходимость лицензии косвенно указывает Положение о лицензировании деятельности по технической защите конфиденциальной информации Утверждено постановлением Правительства Российской Федерации от 15 августа 2006 г. № 504;
- **Обязательного использования сертифицированных СЗИ**

  использование сертифицированных средств заменено на требование использования СЗИ прошедших процедуру оценки соответствия **.**

ЗАКЛЮЧЕНИЕ

СПАСИБО ЗА ВНИМАНИЕ

Презентацию для Вас подготовил

Минченко Александр Владимирович —
начальник отдела технической поддержки
ЗАО «Группа КапиталЪ Управление активами»