Основные положения Доктрины информационной безопасности Российской Федерации.

В декабре 2016 года в России принята новая редакция Доктрины информационной безопасности (Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации", ранее была утверждена Президентом Российской Федерации 9 сентября 2000 г., № Пр-1895).

Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" вступил в силу со дня его подписания.

Текст Указа опубликован на "Официальном интернет-портале правовой информации" (www.pravo.gov.ru) 6 декабря 2016 г., в Собрании законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074

В документ ИБ определена как состояние защищенности национальных интересов в информационной сфере. Под национальными интересами в данном случае понимается совокупность интересов общества, личности и государства, каждая группа интересов необходима для стабильного функционирования социума.

Доктрина – концептуальный документ. Правоотношения, связанные с обеспечением информационной безопасности, регулируются федеральными законами «О государственной тайне», «Об информации», «О защите персональных данных» и другими. На базе основополагающих нормативных актов разрабатываются постановления правительства и ведомственные нормативные акты, посвященные частным вопросам защиты информации. Категории и носители информации Неотъемлемой частью любой информационной системы является информация.

По характеру ограничений (реализации) конституционных прав и свобод в информационной сфере выделяют четыре основных вида правовой (регламентированной законами) информации:
- информация с ограниченным доступом;
- информация без права ограничения; - иная общедоступная информация (например, за деньги);
- информация, запрещенная к распространению.
Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.
К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Владельцем государственной тайны является само государство. Требования по защите этой информации и контроль за их соблюдением регламентируются законом РФ «О государственной тайне». В нем законодательно установлен Перечень сведений,

сопоставляющих государственную тайну, и круг сведений, не подлежащих к отнесению к ней. Предусмотрена судебная защита прав граждан в связи с необоснованным засекречиванием.
Определены органы защиты государственной тайны:
- межведомственная комиссия по защите государственной тайны;
- федеральные органы исполнительной власти, уполномоченные в области:
- обеспечения безопасности - Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- обороны – Министерство обороны;
- внешней разведки – Федеральная служба безопасности (ФСБ обеспечивает, в т.ч. криптографическую защиту);
- противодействия техническим разведкам и технической защиты информации – ФСТЭК; - другие органы.

Конфиденциальная информация – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности. Этой информацией владеют различные учреждения, организации и отдельные индивидуумы.

В Доктрине информационной безопасности Российской Федерации под термином информационная безопасность понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. В более узком смысле, под информационной безопасностью понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений. Защита информации – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах. Информационная безопасность – это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации – это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы2 . Под субъектами информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры. К поддерживающей инфраструктуре относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Ущерб может быть приемлемым или неприемлемым. Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер

ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а целью защиты информации становится уменьшение размеров ущерба до допустимых значений. Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации. Таким образом, концепция информационной безопасности, в общем случае, должна отвечать на три вопроса: - Что защищать? - От чего (кого) защищать? - Как защищать? Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие составляющие: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Иногда в число основных составляющих информационной безопасности включают защиту от несанкционированного доступа (НСД) к информации, под которым понимают доступ к информации, нарушающий правила разграничения доступа с использование штатных средств. В то же время обеспечение конфиденциальности как раз и подразумевает защиту от НСД.