ДОКТРИНА
информационной безопасности Российской Федерации

Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646

1. Гражданский кодекс РФ.
2. Федеральный закон от 29.06.2004 г. № 98-ФЗ «О коммерческой тайне».
3. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 6.04.2011 г. № 63-ФЗ «Об электронной подписи».

Регуляторами в области информационной безопасности в РФ являются: Федеральная служба по техническому и экспортному контролю,
Федеральная служба безопасности, Федеральная служба охраны, Министерство обороны РФ, Министерство связи и массовых коммуникаций
РФ, Служба внешней разведки РФ и Банк России.

Основные термины и понятия информационной безопасности

Информационный ресурс, или информационный потенциал общества, - социально значимая информация, содержащаяся во всех действующих в обществе информационных системах, которая может быть использована для принятия решений во всех сферах человеческой деятельности.

Информация - сведения (сообщения, данные) независимо от формы их представления.

(из Закона РФ **об** *«Информации, информационных технологиях и защите информации)*

Информационное оружие - специально подобранная информация; под ее воздействием происходят изменения в информационных системах и процессах (физических, биологических, социальных) в соответствии с замыслом субъекта его применения.

Информационная война - форма борьбы сторон с использованием специальных способов и средств для воздействия на информационную среду противника и зашиты собственной в интересах достижения поставленных целей.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Фактор, воздействующий на защищаемую информацию - явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость информационной системы (*брешь)*- свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

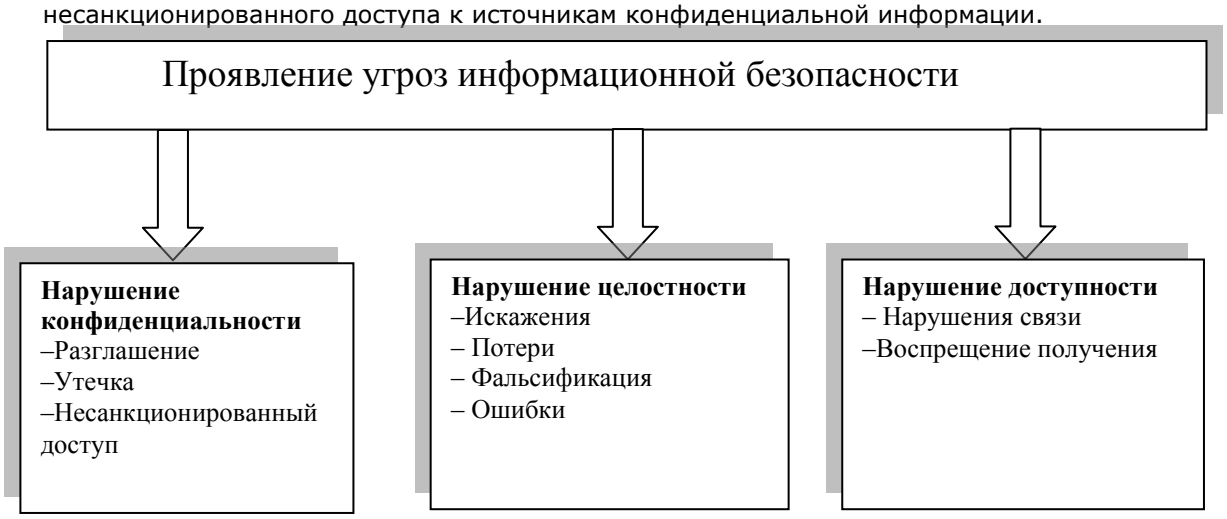
Реализация угроз информационным ресурсам

1. Через имеющиеся агентурные источники в органах государственного управления и коммерческих структурах, имеющих возможность получения конфиденциальной информации (суды, налоговые органы, коммерческие банки и т. д.).

2. Путем подкупа лиц, непосредственно работающих в организации или структурах, напрямую связанных с ее деятельностью.

3. Путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной технике с помощью технических средств разведки и съема информации.

4. Путем прослушивания конфиденциальных переговоров и другими способами несанкционированного доступа к источникам конфиденциальной информации.



Согласно данным Национального института стандартов и технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате **ошибок пользователей и обслуживающего персонала.** Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Угрозы в деятельности предприятий и учреждений:

По отношению к отдельной организации существуют следующие основные **виды внешних угроз:**

1. Недобросовестные конкуренты.

2. Криминальные группы информирования.

3. Противозаконные действия отдельных лиц и организаций административного аппарата, в том числе и налоговых служб.

4. Нарушение установленного регламента сбора, обработки и передачи информации.

Основные виды внутренних угроз:

1. Преднамеренные преступные действия собственного персонала организации.

2. Непреднамеренные действия и ошибки сотрудников.

3. Отказ оборудования и технических средств.

4. Сбои программного обеспечения средств обработки информации.

Соотношение внутренних и внешних угроз в соответствии с характеризуется следующими показателями: 81,7% угроз совершается либо самими сотрудниками организаций, либо при их прямом или опосредованном участии (внутренние угрозы); 17,3% угроз — внешние угрозы или преступные действия; 1,0% угроз — угрозы со стороны случайных лиц.

Объекты угроз в деятельности предприятий организаций

1. Человеческие ресурсы (персонал, сотрудники, компаньоны и др.), включая трудовые и кадровые ресурсы.
2. Материальные ресурсы.
3. Финансовые ресурсы.
4. Временные ресурсы.
5. Информационные ресурсы, включая интеллектуальные ресурсы (патенты, незавершенные проектно-конструкторские разработки, ноу-хау, программные продукты, массивы бухгалтерской и статистической информации и пр.).

Наиболее опасным источником угроз предприятиям выступают собственные сотрудники. Мотивами внутренних угроз в этом случае являются безответственность, некомпетентность (низкая квалификация), личные побуждения (самоутверждение, корыстные интересы).

Недобросовестная конкуренция:

1.Все действия, ведущие к тому, что потребитель может принять предприятие, товары, промышленную или коммерческую деятельность данной организации за предприятие, товары, промышленную или коммерческую деятельность конкурента.

2.Ложные заявления в ходе коммерческой деятельности, дискредитирующие предприятие, товары, промышленную или коммерческую деятельность конкурента.
3.Использование в ходе коммерческой деятельности указаний или обозначений, которые вводят потребителя в заблуждение относительно природы, способа изготовления, характеристик, пригодности для определенных целей или количества товаров.

Реализация угроз в данном случае снижает эффективность и надежность функционирования организаций, а в отдельных случаях, приводят к прекращению их деятельности из-за опасности экономического, социального, правового, организационного, информационного, экологического, технического и криминального характера. Объектами угроз могут быть элементы вещественного, личного («человеческого»), финансового, информационного и иного капитала, составляющего экономическую основу деятельности предпринимательства.

Виды возможных ущербов (потерь):

1.**Материальные виды потерь** проявляются в непредусмотренных предпринимательским проектом дополнительных затратах или прямых потерях оборудования, имущества, продукции, сырья, энергии и т. д.

2.**Трудовые потери** — это потери рабочего времени, вызванные случайными, непредвиденными обстоятельствами; измеряются в часах рабочего времени. Перевод трудовых потерь в денежное выражение осуществляется путем умножения трудочасов на стоимость (цену) одного часа.

3. **Кадровые потери** — потери необходимых предприятию профессиональных, высококвалифицированных работников; измеряются в затратах на подбор и обучение нового кадрового состава в денежном выражении.

4. **Финансовые потери** — прямой денежный ущерб, связанный с непредусмотренными платежами, выплатой штрафов, уплатой дополнительных налогов, потерей денежных средств и ценных бумаг.

5. **Временные потери**. Происходят, когда процесс деятельности организации идет медленнее, чем намечено. Прямая оценка таких потерь осуществляется в часах, днях, неделях, месяцах запаздывания в получении намеченного результата. Чтобы перевести оценку потерь времени в денежное измерение, необходимо установить, к каким потерям дохода, прибыли способны приводить потери времени. В конечном итоге оцениваются в денежном выражении.

6.**Информационные потери**. Одни из самых серьезных потерь в деятельности, способные привести к краху всей организации. Исчисляются в стоимостном выражении.

7.**Особые виды потерь** проявляются в виде нанесения ущерба здоровью и жизни людей, окружающей среде, престижу организации, а также вследствие других неблагоприятных социальных и морально - психологических последствий.

Информационный ущерб (потери) связан с наличием в процессе деятельности организации информационного риска, который входит в общий риск.

Информационный риск - вероятность (угроза) потерь активов субъекта экономики (предпринимателя) в результате потерь, порчи, искажения и разглашения информации.

Информационный риск классифицируется следующим образом:

- риск прерывания информации (прекращение нормальной обработки информации, например, вследствие разрушения, вывода из строя вычислительных средств). Такая категория действий может вызвать весьма серьезные последствия, если даже информация при этом не подвергается никаким воздействиям;
- риск кражи информации (считывание или копирование информации, хищение магнитных носителей информации и результатов печати с целью получения данных, которые могут быть использованы против интересов владельца (собственника) информации);
- риск модификация информации (внесение несанкционированных изменений в данные, направленных на причинение ущерба владельцу (собственнику) информации);
- риск разрушения данных (необратимое изменение информации, приводящее к невозможности ее использования);
- риск электромагнитного воздействия и перехвата информации в автоматизированных и информационных системах (АИС);
- риск съема информации по акустическому каналу;
- риск прекращения питания АИС и поддерживающей инфраструктуры);
- риск ошибки операторов и поставщиков информационных ресурсов АИС;
- риск сбоев программного обеспечения АИС;
- риск неисправности аппаратных устройств АИС (в результате халатных действий сотрудников, несоблюдения техники безопасности, природных катаклизмов, сбоев программных средств и т. д.).

Все противоправные действия приводят к нарушению конфиденциальности, достоверности, целостности и доступности информации.

Общая характеристика основных методов получения информации о различных

сторонах деятельности и перечень используемых при этом технических средств

№	Действия	Физическое явление	Способ (средство) съема информации
1	Разговор нескольких лиц	Акустический сигнал	Подслушивание, в том числе случайное. Диктофоны. Закладные устройства с передачей информации по: имеющимся коммуникациям (трубам, цепям сигнализации, сетям 220 В, телефонным линиям...); специально проложенным проводам; радио- или ИК-каналу Направленные микрофоны
		Виброакустический сигнал	Стетоскоп. Вибродатчик с передачей информации по: радиоканалу; проводам; коммуникациям; ИК-каналу Оптический лазерный микрофон
		Гидроакустический сигнал	Гидроакустический датчик
		Акустоэлектрический сигнал	Радиоприемник спецназначения
		Движение губ	Визуально, в том числе оптическими приборами Камера, в том числе с передачей по проводам и радиоканалу
2	Разговор по телефону	Акустический сигнал	Аналогично п. 1
		Электрический сигнал в линии	Параллельный телефон, прямое подключение, подключение через электромагнитный датчик, телефонная радиозакладка
		Побочные электромагнитные излучения (ПЭМИ) и наводки	Специальные радиотехнические устройства
3	Разговор по радиотелефону	Акустический сигнал Электромагнитные волны	Аппаратура п. 1 Специальные радиоприемные устройства
4	Документ на бумажном носителе	Наличие	Визуально, в том числе с помощью оптических средств Фотографирование, в том числе с дистанционной передачей снимка Копирование
5	Размножение документа на бумажном носителе	Печать документа на принтере	Кража, визуально
		Шумы принтера	Спецаппаратура акустического контроля
		ПЭМИ от ЭВМ	Специальные радиотехнические устройства
6	Почтовые отправления	Наличие	Прочтение: со вскрытием, без вскрытия
	Документ на небумажном носителе	Носитель	Копирование, вскрытие, несанкционированное использование ЭВМ
	Изготовление документа на небумажном носителе	Изображение на дисплее	Визуально, в том числе с помощью оптических средств Фотографирование. Видео- или телевизионные закладные устройства
		ПЭМИ	Специальные радиотехнические устройства
		Электрические сигналы в сетях	Аппаратные закладки
7	Передача документа на небумажном носителе	Электрические сигналы	Несанкционированное подключение, имитация пользователя

Виды защиты информации:

Правовая защита информации - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации - защита информации с помощью ее криптографического преобразования.

Физическая защита информации- защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты. При этом к объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Организационная защита информации – это регламентация деятельности организации и взаимоотношений персонала на нормативно – правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

В соответствии со статьей **128. Гражданского кодекса РФ** к объектам гражданских прав относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права; работы и услуги; **информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность),** нематериальные блага.

Обладатель информации вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Ограничение доступа к информации устанавливается **федеральными законами** в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является **соблюдение конфиденциальности информации**, доступ к которой ограничен федеральными законами.

Информация **в зависимости от категории доступа** к ней подразделяется на:

- общедоступную информацию;
- информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация **в зависимости от порядка ее предоставления или распространения** подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в РФ ограничивается или запрещается.