ЧАСТЬ I

Позвольте Вас познакомить...

В этой части

- *Информационная безопасность государства*
- *Информационная система как объект защиты*
- *Безопасность в Internet*
- *Принципы построения систем защиты информации*

Информационная безопасность государства

1

В этой главе

- *Государственная политика обеспечения информационной безопасности*
- *Ключевые проблемы информационной безопасности государства*
- *Основные задачи обеспечения безопасности информации*
- *Развитие научно-практических основ информационной безопасности*
- *Современные методы обеспечения информационной безопасности*
- *Безопасность информационных ресурсов*
- *Права на доступ к информации*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Информацию без преувеличения можно отнести к одному из решающих ресурсов развития. Она в современном мире активно влияет на все сферы жизнедеятельности не только отдельных государств, но и всего мирового сообщества. Однако в определенных случаях информация может быть использована не только во благо, но и во вред интересам личности, общества и государства. Поэтому роль информационной безопасности в системе национальной безопасности не только существенно возрастает, но и выходит на первый план.

Национальный информационный ресурс стал одним из главных источников экономической мощи как государства в целом, так и отдельных финансовых, научно-исследовательских и производственных субъектов. В этой связи необходимо сформулировать государственные интересы в информационной сфере, провести оценку эффективности существующей системы безопасности и наметить первоочередные меры по ее совершенствованию.

Государственная информационная политика должна предусмотреть не только права граждан, юридических лиц и государства на свободное получение, распространение и использование информации, но и учесть необходимость защиты государственных информационных ресурсов, конфиденциальной информации и интеллектуальной собственности.

Государственная политика обеспечения информационной безопасности (003)

Необходимо учитывать следующие основные принципы государственной политики обеспечения информационной безопасности.

1. Государственная политика должна обеспечить безусловное правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом. В этих целях государство совершенствует существующее и разрабатывает новое законодательство и формирует нормативно-правовую базу информационных отношений в обществе, осуществляет контроль за безусловным исполнением законов и нормативно-правовых актов.

2. Государство исходит из того, что информационные ресурсы являются объектом собственности, и способствует введению их в хозяйственный оборот.

3. Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и средств, способных обеспечить создание национальных телекоммуникационных сетей и включение в мировые информационные сети и системы мониторинга.

4. Государственная политика предусматривает согласованность решений, принимаемых органами власти и местного самоуправления для обеспечения информационной безопасности в рамках единого информационного пространства. Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности.

Основные положения государственной политики (003)

Основные положения государственной политики обеспечения информационной безопасности таковы:

- ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;
- ответственность за сохранность, засекречивание и рассекречивание информации персонифицируется;
- доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;
- государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;
- юридические и физические лица, собирающие, накапливающие и обрабатывающее персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;
- государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;
- государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;
- государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

- государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- государство стремится к отказу от зарубежных информационных технологий для информатизации органов власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

Государство обеспечивает защиту общества от ложной, искаженной и недостоверной информации...

- государство формирует программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности;
- государство прилагает усилия для противодействия информационной экспансии других стран, поддерживает интернационализацию глобальных информационных сетей и систем.

Ключевые проблемы информационной безопасности государства

Обеспечение информационной безопасности государства требует:

- Развития научно-практических основ информационной безопасности, соответствующей современной геополитической ситуации и условиям политического и социально-экономического развития государства.
- Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработки реестра информационного ресурса, регламента информационного обмена, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.
- Разработки механизмов реализации прав граждан на информацию.
- Формирования системы информационной безопасности, являющейся составной частью общей системы национальной безопасности страны.
- Разработки современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации.
- Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.
- Исследования форм и способов цивилизованного воздействия государства на формирование общественного сознания.
- Комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Основные направления деятельности государства в области информационной безопасности (001)

Перечислим основные направления этой деятельности.

Развитие научно-практических основ информационной безопасности (001)

- Разработка стратегии обеспечения информационной безопасности страны.
- Обоснование государственной политики в условиях глобализации информационных процессов, формирования мировых информационных сетей, стремления некоторых стран к доминированию в развитии и использовании мирового информационного пространства.
- Разработка научно-практических основ формирования и проведения государственной политики в области обеспечения информационной безопасности.
- Обоснование приоритетов национальной безопасности, соответствующих долговременным интересам общественного развития.

Развитие законодательной и нормативно-правовой базы обеспечения информационной безопасности (001)

Определение порядка разработки законодательных и нормативно-правовых актов, а также механизмов практической реализации принятого законодательства, а именно:

Разработка нормативно-правовых и организационно-методических документов, регламентирующих:

- деятельность в области информационной безопасности органов государственной власти;
- взаимоотношения субъектов информационной деятельности в части обеспечения информационной безопасности;
- регулирование государством процессов функционирования и развития рынка средств информации, информационных продуктов и услуг;
- информационные отношения в обществе и государстве в условиях рыночной экономики.

Разработка концепции информационной безопасности, специальных правовых и организационных мероприятий, обеспечивающих сохранение и развитие информационных ресурсов.

Формирование правового статуса субъектов системы информационной безопасности, пользователей информационных и телекоммуникационных систем; определение их ответственности за обеспечение информационной безопасности процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и нарушившим регламент информационных воздействий, а также правонарушения с использованием незащищенных средств информации, разработку состава правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Разработка законодательных и нормативных актов, регулирующих порядок:

- ликвидации последствий воздействий угроз информационной безопасности;
- восстановления нарушенного права и ресурсов;
- реализации компенсационных мер.

Совершенствование форм и методов предотвращения угроз информационной безопасности (003)

- Разработка нормативно-правовой базы функционирования системы информационной безопасности, разграничение полномочий органов государственной власти и управления по обеспечению информационной безопасности.
- Разработка системы мониторинга состояния информационной безопасности.
- Разработка предложений по созданию благоприятных условий по выводу из критического состояния отечественных отраслей промышленности, производящих средства информатизации и защиты информации.
- Анализ технико-экономических параметров отечественных и зарубежных программно-технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники.
- Разработка системы экономических и статистических показателей, характеризующих эффективность функционирования системы обеспечения информационной безопасности; исследование критериев и методов оценки эффективности системы информационной безопасности.

Развитие современных методов обеспечения информационной безопасности (003)

- Разработка форм и способов цивилизованного воздействия государства на формирование общественного сознания.
- Разработка методов комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.
- Разработка практических рекомендаций по сохранению и укреплению политической стабильности в обществе; обеспечению прав и свобод граждан; укреплению законности и правопорядка методами информационной безопасности.
- Формирование подходов и способов обеспечения органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией.
- Разработка основных направлений деятельности по предотвращению негативных информационных воздействий на индивидуальное, групповое и общественное сознание.

Мониторинг состояния информационной безопасности...

- Разработка цивилизованных, демократических форм и методов воздействия на средства массовой информации.
- Разработка механизмов развития информационных отношений в сфере предпринимательства и включения информационного ресурса в хозяйственный оборот.
- Исследование основных путей ослабления криминогенной обстановки, снижения числа компьютерных преступлений, в первую очередь — в кредитно-финансовой сфере.
- Разработка методов и практических рекомендаций по контролю за экспортом отечественных наукоемких технологий.
- Обоснование направлений противодействия "информационному оружию".
- Совершенствование способов контроля за персоналом в защищенных информационных системах.

Основные задачи обеспечения безопасности информации (002)

Для эффективного обеспечения безопасности информации требуется создание развитого методологического базиса, позволяющего решить следующие комплексные задачи:

- создать систему органов, ответственных за безопасность информации;
- разработать теоретико-методологические основы обеспечения безопасности информации;
- решить проблему управления защитой информации и ее автоматизации;
- создать нормативно-правовую базу, регламентирующую решение всех задач обеспечения безопасности информации;
- наладить производство средств защиты информации;
- организовать подготовку специалистов по защите информации;
- подготовить нормативно-методическую базу для проведения работ по обеспечению БИТ.

Более подробно цели и содержание перечисленных задач приведены в таблице 1.1.

Безопасность информационных ресурсов

Государственная политика в сфере формирования информационных ресурсов и информатизации должна быть направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития страны.

Основными направлениями государственной политики в сфере информатизации являются:

- обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;
- формирование и защита государственных информационных ресурсов;
- создание и развитие и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве;
- создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, организаций и общественных объединений на основе государственных информационных ресурсов;
- обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан и организаций в условиях информатизации;
- содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий и средств их обеспечения;
- формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;
- поддержка проектов и программ информатизации;
- создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;
- развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Таблица 1.1. Комплексные задачи обеспечения безопасности информации.

п/п	*Задачи*	*Цели решения*	*Общее содержание*
1	Создание *системы органов,* ответственных за безопасность иинформации	Создание стройной системы органов, необходимых и достаточных для эффективного решения всех задач обеспечения безопасности информации на общегосударственном, региональном (ведомственном) и объектовом уровнях	Создание органов, осуществляющих: 1) управление процессами обеспечения безопасности; 2) проведение НИР и ОКР; 3) разработку и производство необходимых средств; 4) практическое решение задач обеспечения безопасности информации на обьектах; 5) подготовку, повышение квалификации и переподготовку кадров
2	Разработка *теоретико-методологического базиса* обеспечения безопасности информации	Создание научно обоснованного базиса решения всех задач, связанных с обеспечением безопасности информации	1. Обоснование понятийого аппарата 2. Аналитико-синтетическаяобработка имеющихся данных 3. Обоснование современной постановки задачи 4. Обоснование стратегических подходов к обеспечению безопасности 5. Разработка методов решения задач обеспечения безопасности 6. Обоснование структуры и содержания инструментально-методологической базы решения задач 7. Обоснование путей и способов решения задач обеспечения безопасности 8. Обоснование перспектив развития теории и практики обеспечения безопасности информации
3	Решение проблемы *управления защитой* информации и ее автоматизации	Разработка методов и технологии управления защитой информации	1. Отработка принципов управления в рамках государственной СЗИ: 1) по трем основным уровням: ◆ во взаимодействии со структурами государственной власти; ◆ в регионах, территориально-промышленных зонах; ◆ на предприятиях, полигонах, объектах, в системах и комплексах; 2) в двух состояниях (режимах) ◆ повседневном (режим заблаговременного, планового осуществления мер по ЗИ); ◆ ”быстрого реагирования” (режим принятия оперативных решений и осуществления мер по ЗИ); 2. Создание систем управления защитой информации различного уровня и назначения
4	Создание *нормативно-правовой базы*, регламентирующей решение задач обеспечения безопасности информации	Создание условий, необходимых для правового и нормативного регулирования решения всех задач обеспечения безопасности информации	1. Обоснование структуры и содержания нормативно-правовой базы 2. Разработка и организация принятия законов, регламентирующих деятельность в области обеспечения безопасности информации 3. Разработка, утверждение и распространение системы общегосударственных руководящих и методических материалов по обеспечению безопасности информации 4. Определение порядка разработки, утверждения региональных (ведомственных) документов по обеспечению безопасности информации

Таблица 1.1. Комплексные задачи обеспечения безопасности информации (продолжение).

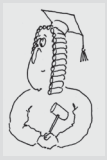
n/n	*Задачи*	*Цели решения*	*Общее содержание*
			5. Разработка, утверждение и распространение комплекта типовых инструкций по решению задач обеспечения безопасности информации 6. Разработка и узаконивание правил сертификации средств и лицензирования деятельности по обеспечению безопасности информации
5	Организация производства *средств защиты* информации на промышленной основе	Создание индустрии производства и распространения средств обеспечения безопасности информации	1. Обоснование перечня и содержания средств обеспечения безопасности 2. Создание системы предприятий и учреждений, производящих средства обеспечения безопасности 3. Определение порядка разработки, аттестации и распространения технических средств 4. Определение порядка разработки, аттестации и распространения программных средств 5. Определение порядка разработки, аттестации и распространенния организационных средств 6. Определение порядка разработки, аттестации и распространения криптографических средств
6	Организация системы *подготовки кадров* по безопасности	Создание регулярной системы подготовки специалистов по безопасности информации, необходимого количества и требуемых профилей	1. Разработка и научное обоснование концепции подготовки кадров по безопасности информации 2. Определение перечня учебных заведений, уполномоченных готовить кадры по безопасности информации, и распределение между ними функций 3. Организация подготовки молодых специалистов 4. Организация повышения квалификации специалистов по безопасности информации 5. Организация переподготовки специалистов другого профиля 6. Организация подготовки научно-педагогических кадров в области безопасности информации 7. Организация всеобуча по безопасности информации
7	Создание системы *документационно-методического обеспечения* работ по безопасности информации	Создание регулярной системы обеспечения всех органов и специалистов по безопасности информации необходимыми источниками и пособиями	1. Разработка и научное обоснование системы документационно-методического обеспечения 2. Создание системы разработки, издания и распространения официальных документов 3. Создание системы разработки, издания и распространия трудов монографического характера 4. Создание системы разработки, издания и распространения учебно-методической литературы 5. Создание системы разработки, издания и распространения периодических изданий

Документирование информации (101)

Документирование информации — обязательное условие включения информации в информационные ресурсы, которое осуществляется в порядке, установленном органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов.

Документ, полученный из информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законом. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и при соблюдении установленного режима их использования. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии.



Определение

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и т.д.).

Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Права собственности на информационные ресурсы регулируются соответствующим гражданским законодательством.

Информационные процессы – процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Физические и юридические лица являются собственниками тех документов (массивов документов), которые созданы на их средства, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти. Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо от их организационно-правовой формы и форм собственности, а также гражданами на основании закона, формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию.

Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных соответствующим законодательством. Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

Информационные ресурсы могут быть товаром...

Государственные информационные ресурсы (101)

Формирование государственных информационных ресурсов осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Документы, принадлежащие физическим и юридическим лицам, могут быть включены по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

Государственные информационные ресурсы — открыты и общедоступны. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти.

Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований. Собственник или владелец документированной информации может обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

Собственник информационных систем или уполномоченные им лица в соответствии с законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

Владелец информационных систем обеспечивает уровень защиты информации в соответствии с законодательством.

Риск, связанный с использованием не сертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из не сертифицированной системы, лежит на потребителе информации.

Защита прав субъектов в сфере формирования информационных ресурсов, пользования ими, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и на граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров.

Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

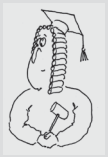
Виновные в незаконном ограничении доступа к информации несут ответственность...

Руководители и другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность согласно уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Информация о гражданах (персональные данные) (101)

Персональные данные относятся к категории конфиденциальной информации. Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную или семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации их прав и свобод. Ограничение прав граждан на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.



Определение

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

Информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

Информация о гражданах (персональные данные) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом;

Пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

При решении правовых вопросов в процессе внедрения современных информационных технологий, нельзя забывать о возможных нарушениях законных прав и интересов граждан в силу недобросовестного поведения пользователей таких систем.

Персональные данные относятся к категории конфиденциальной информации...

Процесс совершенствования демократии предполагает дальнейшее развитие системы гарантий прав личности от возможных злоупотреблений со стороны должностных лиц. Тем более, что в области охраны информации о личности еще имеются пробелы.

Разумеется, тенденция к расширению количества видов информации о личности, накапливаемых банками данных, носит объективный характер, обусловлена возрастанием роли информации в решении масштабных производственных и социально-культурных задач. Однако очевидно, что собираемые данные должны быть ограничены в виду реальной возможности нанесения вреда законным интересам граждан, о которых информация собирается.

Появление информационных систем, накапливающих огромные массивы персональных данных, позволяет достаточно конкретно создавать образ человека и разрабатывать соответствующую систему контроля за ним. И не только за отдельным человеком, но и за группой людей.

В результате ставится под сомнение общепринятый принцип “презумпции невиновности”, так как человек, за которым ведется наблюдение незаконно, без его ведома, попадает в положение подозреваемого или даже обвиняемого.

Права на доступ к информации из информационных ресурсов (101)

Пользователи — граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения — обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения зап-

рашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации. Источником прибыли в этом случае является результат труда и вложенных средств при создании производной информации, но не исходная информация.

В плане взаимосвязи обеспечения и законности реализации прав и свобод граждан, а также использования возможностей ИС, следует обратить внимание на опыт развитых стран в этой сфере отношений. Так, Конгрессом США были приняты соответствующие законы, позволяющие гражданам, средствам массовой информации и частным организациям знакомиться с информацией правительственных учреждений.

Право граждан затребовать информацию касается документации органов исполнительной власти: министерств, административных и военных ведомств, правительственных корпораций и иных учреждений. Под действие этих законов не подпадает документация таких выборных должностей, как президент, вице-президент, сенаторы и члены Палаты представителей Конгресса.

Кроме того, закон о свободе информации установил ряд ограничений на общие правила, оговорив конкретные ***категории информации, не выдаваемой гражданам по их запросам***. Это:

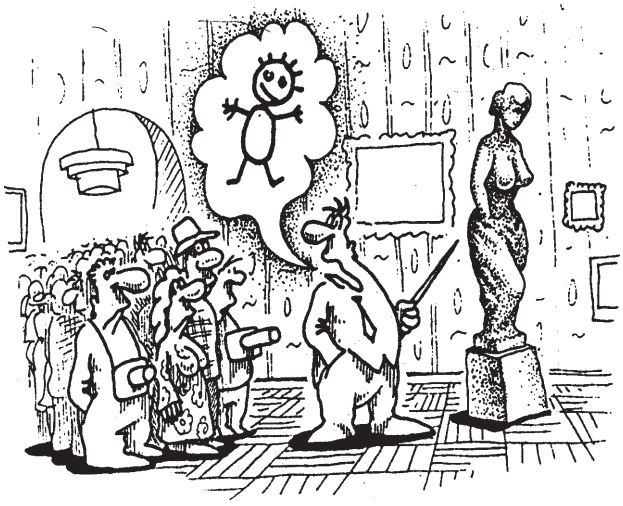
- засекреченные документы;
- внутриведомственные служебные правила, инструкции, предписания;
- информация, не подлежащая разглашению в соответствии с другими законодательными актами;
- конфиденциальная деловая информация (коммерческая и финансовая информация о предпринимательской деятельности частных лиц и корпораций);
- внутриведомственная служебная корреспонденция;
- информация, затрагивающая частную жизнь граждан;
- информация об оперативной и следственной работе правоохранительных органов;
- информация финансовых учреждений.

В тех случаях, когда использование информации может повлечь лишение гражданина прав, льгот или привилегий, гарантируемых программами социальной помощи, учреждение должно получать информацию по возможности непосредственно от гражданина.

Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные массивы и вид информации, в соответствии с их компетенцией, либо непосредственно ее собственником, в соответствии с законодательством.

Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных законами.

Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных соответствующим законодательством или собственником этих информационных ресурсов, в соответствии с законодательством. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном соответствующим законодательством.



Граждане имеют право на доступ к информации о них...

Резюме

***Обеспечением информационной безопасности государства требует решения следующих ключевых проблем*:**

1. Развития научно-практических основ информационной безопасности, отвечающей современной геополитической ситуации и условиям политического и социально-экономического развития государства.

2. Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

3. Разработки механизмов реализации прав граждан на информацию.

4. Формирования системы информационной безопасности, являющейся составной частью общей системы национальной безопасности страны.

5. Разработки современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

7. Исследований форм и способов цивилизованного воздействия государства на формирование общественного сознания.

8. Комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Для эффективного обеспечения безопасности информации требуется создание развитого методологического базиса, позволяющего решить следующие комплексные задачи:

- создать систему органов, ответственных за безопасность информации;
- разработать теоретико-методологические основы обеспечения безопасности информации;
- решить проблему управления защитой информации и ее автоматизации;
- создать нормативно-правовую базу, регламентирующую решение всех задач обеспечения безопасности информации;
- наладить производство средств защиты информации;
- организовать подготовку специалистов по защите информации;
- подготовить нормативно-методическую базу для проведения работ по обеспечению БИТ.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти.

Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.