Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
«Уральский государственный педагогический университет»

В. В. Гафнер

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Часть 1

Екатеринбург 2009

УДК 347-049.5(075.8)
ББК Ц9я7
Г 24

Рецензенты:
Репин Ю.В., кандидат педагогических наук, профессор, заведующий кафедрой безопасности жизнедеятельности, декан факультета безопасности жизнедеятельности Уральского государственного педагогического университета

Сапронов В.В., кандидат технических наук, профессор Московского государственного университета культуры и искусств, директор Института безопасности жизнедеятельности (сфера образования) Фонда национальной и международной безопасности

Чеурин Г.С., научный руководитель муниципального образовательного учреждения «Центр экологического выживания и безопасности» (г. Екатеринбург), руководитель учебного центра по предотвращению социальных и природных чрезвычайных ситуаций ООО «ТМО «ИТАЛЛ», руководитель молодёжной учебно-оздоровительной экспедиции «Сибирский путь», действительный член географического общества России, почетный полярник

Гафнер В. В.

Г 24 Информационная безопасность: учебное пособие в 2 ч. / В. В. Гафнер ; ГОУ ВПО «Урал. гос. пед. ун-т». – Екатеринбург, 2009. – Ч.1. – 155 с.

ISBN 978-5-7186-0414-6

Учебное пособие «Информационная безопасность» предназначено для студентов педагогических ВУЗов, обучающихся по специальности 050104 – Безопасность жизнедеятельности. В пособии рассматриваются теоретические и практические аспекты обеспечения информационной безопасности в мирное и военное время, а также в условиях чрезвычайных ситуаций. Значительное место уделяется социальным аспектам информационной безопасности, влиянию информации на жизнь и деятельность людей.

Пособие может быть полезно специалистам в области безопасности жизнедеятельности, учителям ОБЖ, учащимся, родителям.

УДК 347-049.5(075.8)
ББК Ц9я7

ISBN 978-5-7186-0414-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Учебная дисциплина «Информационная безопасность» включает в себя теоретические и практические аспекты обеспечения информационной безопасности в мирное и военное время, а также в условиях чрезвычайных ситуаций. Основная цель этой дисциплины заключается в формировании системы знаний об информационной безопасности личности, организации, общества, государства и основных мерах по её обеспечению. Дисциплина носит междисциплинарный характер и тесно связана с другими дисциплинами специальности «Безопасность жизнедеятельности»: теоретические основы безопасности человека, основы национальной безопасности, правовое регулирование и органы обеспечения безопасности жизнедеятельности, опасности социального характера и защита от них, криминальные опасности и защита от них, психологические основы безопасности.

Учебное пособие подготовлено в соответствии с положениями Государственного образовательного стандарта высшего профессионального образования по специальности 050104 – «Безопасность жизнедеятельности», дисциплина ДПП. Ф16. «Информационная безопасность» (федеральный компонент).

Предполагается, что в результате изучения этой дисциплины студенты получат знания:

- о понятиях информационной безопасности;
- о видах и источниках опасностей и угроз в сфере информационных процессов и систем;
- о нормативных актах, обеспечивающих информационную безопасность;
- об основах государственной политики обеспечения информационной безопасности;
- о методах и средствах обеспечения информационной безопасности в мирное и военное время, а также в условиях чрезвычайных ситуаций;
- о методах и средствах ведения современной информационно-психологической войны.

Успешно изучившие данную дисциплину будут уметь:

- защищаться от негативного информационного воздействия;

- принимать решения на основе анализа и оценки информации;

- применять полученные знания в самостоятельной педагогической деятельности;

- формировать у учащихся знания и умения в области информационной безопасности.

Отличие настоящего учебного пособия от имеющейся учебной литературы по информационной безопасности заключается в том, что его основное содержание посвящено социальным аспектам информационной безопасности, влиянию информации на жизнь и деятельность людей.

В первой части пособия рассматривается значение информации в современном мире и образовании, основы правового обеспечения информационной безопасности, а также меры по обеспечению информационной безопасности РФ.

Во второй части пособия рассмотрены вопросы обеспечения информационной безопасность человека в повседневной жизни и в чрезвычайных ситуациях, представлены методы и средства защиты информации. Отдельными разделами представлены информационные и психологические войны, а также информационная преступность.

Текст пособия подробно структурирован. Все разделы снабжены соответствующими подзаголовками. В конце пособия приведён словарь основных терминов, содержащий их наиболее употребительные толкования.

ГЛАВА 1. ЗНАЧЕНИЕ ИНФОРМАЦИИ В СОВРЕМЕННОМ МИРЕ И ОБРАЗОВАНИИ

1.1. Понятие информации и информационной безопасности

Понятие информации. Виды и свойства информации. Структура информационного процесса. Понятие информационной безопасности. Информационные опасности и угрозы. Принципы обеспечения информационной безопасности.

Основные термины и понятия:
Данные
Доступность информации
Защита информации
Знания
Информатизация
Информационная безопасность
Информация
Конфиденциальность информации
Целостность информации

Понятие информации

Информация является одним из фундаментальных понятий современности и относится к разряду тех, которые имеют очень широкое употребление. Информационные взаимодействия – это основа существования как живой, так и неживой природы. Без информационных процессов немыслима и социальная жизнь. Информационные технологии представляют собой основу современной и особенно зарождающейся цивилизации – информационного общества.

Термин «информация» происходит от латинского слова «***informatio***», что означает *сведения, разъяснения, изложение*. Обычно под информацией понимаются знания, сведения, данные, сообщения и сигналы, с которыми мы имеем дело в повседневной жизни и проявление которых мы наблюдаем в природе и обществе.

Определение информации, которое содержится в энциклопедическом словаре, говорит о том, что «**информация** – *это общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом,*

обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму».

Правовое определение «информации» ввёл Федеральный закон (ФЗ) «Об информации, информатизации и защите информации». В соответствии с ним «**информация** – *это сведения о лицах, предметах, фактах, событиях, процессах независимо от формы их представления*». Позже этот ФЗ утратил силу и его преемником стал ФЗ «Об информации, информационных технологиях и о защите информации». В новом законе интересующее нас определение было немного изменено: «**информация** – *сведения (сообщения, данные) независимо от формы их представления*».

В научной литературе можно встретить десятки попыток дать определение «информации». Многие специалисты признают, что даже достаточно полного, не говоря уж о всеобъемлющем, определения информации дать невозможно, что в каждой научно-прикладной ситуации её определение имеет «своё лицо» и выполняет свои функции.

В философских работах развиваются представления об информации как о некой фундаментальной субстанции, стоящей в одном ряду с материей и энергией, или о том, что информационные взаимодействия – это всего лишь некие формы процессов «отражения», присущих как материальному, так и духовному миру.

В естественных науках под информацией, как правило, понимаются знания об объектах и процессах окружающего нас мира ранее получателю неизвестные. В процессе познания именно информация представляет собой «нечто», что заставляет «подправлять», умножать наши знания. Естественно, что ценность её всегда весьма субъективна и во многом определяется возможностями потребителя, его целями, степенью его восприимчивости и уровнем его познаний.

В наше время существует несколько подходов к определению понятия «информация». В связи с развитием средств связи, телекоммуникаций, вычислительной техники, их использованием для обработки и передачи информации, возникла необходимость измерять её количественные характеристики. Так, в первом подходе различают разные измерения (меры) информации и понятие «информация» может наполняться новым содержанием:

- *техническая мера* − информация, которая передается по телеграфным линиям и отображается на экранах радиолокаторов.

Количество такой информации может быть точно вычислено, и процессы, происходящие с такой информацией, подчиняются физическим законам. По сути, при таком измерении информация отождествляется с данными;

- *семантическая*, т.е. смысловая, мера – та информация, которая содержится, к примеру, в литературном произведении. По существу, при таком подходе информация отождествляется со сведениями и фактами.

Другой подход состоит в том, что информация – это характеристика, такая же, как, например, энергия или масса в физике. Определенным образом и в определенных условиях информация равным образом описывает как процессы, происходящие в естественных физических системах, так и процессы, происходящие в искусственно созданных системах.

Сторонники третьего подхода считают, что информация как объект едина, но количественные оценки могут быть разными. Отдельно следует вводить количество информации − строгую оценку, для которой можно развивать единую формальную теорию. Кроме количества информации следует оценивать ещё и качественные её показатели, которые в конечном итоге определяют ценность информации: достоверность, актуальность, надёжность.

Учитывая сказанное выше, остановимся на следующем определении:

> **Информация** – *сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.*

Информация может существовать в виде текстов, рисунков, чертежей, фотографий, световых или звуковых сигналов, радиоволн, электрических и нервных импульсов, магнитных записей, жестов и мимики, запахов и вкусовых ощущений, хромосом, посредством которых передаются по наследству признаки и свойства организмов, и т. д.

На практике часто отождествляются определения таких понятий, как «информация», «данные», «знания». Однако эти понятия необходимо различать.

Данные – *фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.*

Данные несут в себе сведения о событиях, произошедших в материальном мире, и являются регистрацией сигналов, возникших в результате этих событий. Однако данные не тождественны информации. Станут ли данные информацией – зависит от того, известен ли метод преобразования данных в известные понятия.

Например, мы можем услышать речь обращающегося к нам человека, говорящего на иностранном и незнакомом нам языке. С одной стороны, мы получили от него данные в виде звуков, но с другой – никакой информации от него мы получить не смогли, т.к. не сумели понять передаваемые нам данные. Они для нас были закодированы, а метода раскодирования мы не знали.

Знание – *форма существования и систематизации результатов человека.*

Информацию человек может получать откуда угодно, а знания приходят тогда, когда человек использует эту информацию и сочетает ее со своим собственным опытом. Информация становится знанием, когда она переработана и проанализирована человеческим мозгом. Знание существует только благодаря людям. Знание – это осознание, понимание и толкование определенной информации с учетом путей наилучшего ее использования для достижения конкретных целей. Знания должны иметь структуру, связь между собой, а не быть хаотичными. Очень важно постоянно их использовать и пополнять.

Выделяют различные виды знания: научное, обыденное (здравый смысл), интуитивное, религиозное и др. Обыденное знание служит основой ориентации человека в окружающем мире, основой его повседневного поведения и предвидения, но обычно содержит ошибки, противоречия. Научному знанию присущи логическая обоснованность, доказательность,

воспроизводимость результатов, проверяемость, стремление к устранению ошибок и преодолению противоречий.

Можно сделать вывод, что фиксируемые воспринимаемые факты окружающего мира представляют собой данные. При использовании данных в процессе решения конкретных задач – появляется информация. Результаты решения задач, истинная, проверенная информация (сведения), обобщенная в виде законов, теорий, совокупностей взглядов и понятий представляют собой знания.

Виды и свойства информации

Информацию можно упорядочить по ряду признаков, т.е. провести ее классификацию. В связи с этим, информация может быть классифицирована следующим образом:

1. По способам восприятия:

Визуальная

Аудиальная

Тактильная

Обонятельная

Вкусовая

2. По форме представления:

Буквенная

Цифровая

Графическая

Кодированная

Комбинированная

3. По форме передачи:

Вербальная (словесная, звуковая)

Невербальная (представленная на определенном носителе: бумаге, дискете и т.д.)

Письменная

Печатная

Телефонная

Электронная

Спутниковая и т.д.

4. По назначению:

Экономическая

Техническая

Социальная

Организационная и т.д.

5. По общественному значению:

5.1. Массовая

Обыденная

Общественно-политическая

Эстетическая

5.2.Личная

Знания

Интуиция

5.3. Специальная

Научная

Производственная

Техническая

Управленческая

6. По изменчивости во времени:

Условно-постоянная (например, место жительства человека)

Условно-переменная (например, последовательность календарных месяцев)

Постоянная (например, дата рождения человека)

Переменная

7. По режиму передачи от одного потребителя информации другому:

В произвольные сроки

По запросу

Принудительно в определенные сроки.

Как и всякий объект, информация обладает **свойствами**. Информация отличается от других объектов природы и общества характерной особенностью: на свойства информации влияют как свойства исходных данных, составляющих ее содержательную часть, так и свойства методов, фиксирующих эту информацию.

Можно выделить 3 группы свойств информации:

1. Атрибутивные свойства – свойства, без которых информация не существует.

2. Прагматические свойства – свойства, которые характеризуют степень полезности информации для пользователя, потребителя и практики.

3. Динамические свойства – свойства, которые характеризуют изменение информации во времени.

Рассмотрим подробнее указанные группы свойств информации.

Атрибутивные свойства информации.

Дискретность. Информацию характеризуют отдельные фактические данные, закономерности и свойства изучаемых объектов, которые распространяются в виде различных сообщений, состоящих из линии, составного цвета, буквы, цифры, символа, знака.

Неотрывность информации от физического носителя и языковая природа информации. Однако, информация не связана жестко ни с конкретным языком, ни с конкретным носителем.

Непрерывность. Информация имеет свойство сливаться с уже зафиксированной и накопленной ранее, тем самым, способствуя поступательному развитию и накоплению.

Передаваемость информации с помощью каналов связи (в том числе с помехами) хорошо исследована в рамках теории информации К. Шеннона. В данном случае имеется ввиду несколько иной аспект: способность информации к копированию, т.е. к тому, что она может быть «запомнена» другой системой и при этом останется тождественной самой себе. Очевидно, что количество информации не должно возрастать при копировании.

Воспроизводимость информации тесно связана с ее передаваемостью и не является ее независимым базовым свойством. Если передаваемость означает, что не следует считать существенными пространственные отношения между частями системы, между которыми передается информация, то воспроизводимость характеризует неиссякаемость и неистощимость информации, т.е. при копировании информация остается тождественной самой себе.

Преобразуемость – фундаментальное свойство информации. Оно означает, что информация может менять способ и форму своего существования.

Копируемость есть разновидность преобразования информации, при котором ее количество не меняется. В общем случае количество информации в процессах преобразования меняется, но возрастать не может.

Прагматические свойства информации.

Адекватность – степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных

или недостоверных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

Актуальность – степень соответствия информации текущему моменту времени. Актуальность – важность для настоящего времени, злободневность, насущность. Только вовремя полученная информация может быть полезна.

Доступность – свойство информации, характеризующее возможность ее получения данным потребителем. Отсутствие доступа к данным или соответствующих методов обработки данных приводит к одинаковому результату: информация оказывается недоступной.

Достоверность. Информация достоверна, если она отражает истинное положение дел. Объективная информация всегда достоверна, но достоверная информация может быть как объективной, так и субъективной. Достоверная информация помогает принять нам правильное решение. Недостоверной информация может быть по следующим причинам:

- преднамеренное искажение (дезинформация) или непреднамеренное искажение субъективного свойства;

- искажение в результате воздействия помех («испорченный телефон») и недостаточно точных средств ее фиксации.

Защищенность – свойство, характеризующее невозможность несанкционированного использования или изменения информации.

Объективность и субъективность. Объективный – существующий вне и независимо от человеческого сознания. Информация – это отражение внешнего объективного мира. Информация объективна, если она не зависит от методов ее фиксации, чьего-либо мнения, суждения. Понятие объективности информации является относительным, т.к. методы являются субъективными. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективный элемент. Объективную информацию можно получить с помощью исправных датчиков, измерительных приборов. Отражаясь в сознании конкретного человека, информация перестает быть объективной, т.к., преобразовывается (в большей или меньшей степени) в зависимости от мнения, суждения, опыта, знаний конкретного субъекта. В ходе информационного процесса степень объективности

информации всегда понижается. Это свойство учитывают, например, в правовых дисциплинах, где по-разному обрабатываются показания лиц, непосредственно наблюдавших события или получивших информацию косвенным путем (посредством умозаключений или со слов третьих лиц).

Полезность. Уменьшение неопределенности сведений об объекте. Полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью. Дезинформация расценивается как отрицательные значения полезной информации.

Полнота. Характеризует качество информации и определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Неполная информация может привести к ошибочному выводу или решению.

Релевантность – способность информации соответствовать нуждам (запросам) потребителя.

Смысл и новизна. Информация перемещается в социальных коммуникациях (взаимодействиях потребителей) и выделяется та ее часть, которая нова для потребителя.

Точность информации определяется степенью ее близости к реальному состоянию объекта, процесса, явления и т. п.

Ценность. Ценность информации различна для различных потребителей и пользователей. Самая ценная информация – объективная, достоверная, полная, и актуальная. При этом следует учитывать, что и необъективная, недостоверная информация (например, художественная литература), имеет большую значимость для человека.

Эргономичность – свойство, характеризующее удобство формы или объема информации с точки зрения данного потребителя.

Динамические свойства информации.

Кумулятивность (от лат. cumulatio – увеличение, скопление) характеризует накопление и хранение информации.

Рост информации. С течением времени количество информации растет, информация накапливается, происходит ее систематизация, оценка и обобщение.

Старение. Информация подвержена влиянию времени. Старение информации заключается в уменьшении ее ценности с течением времени. Старит информацию не само время, а появление новой информации, которая уточняет, дополняет или

отвергает полностью или частично более раннюю. Научно-техническая информация стареет быстрее, эстетическая (произведения искусства) – медленнее.

Стираемость. Это свойство связано с таким преобразованием информации (передачей), при котором ее количество уменьшается и становится равным нулю.

Запоминаемость. С запоминаемой информацией мы имеем дело в реальной практике.

Структура информационного процесса

Те предметы или устройства, от которых человек может получить информацию, называют **источниками** информации.

Те предметы или устройства, которые могут получать информацию, называют **приёмниками** информации.

При переносе информации в виде сигнала от источника к приёмнику (потребителю) она проходит последовательно следующие фазы (говорят – фазы обращения), составляющие информационный процесс:

1. Восприятие (если фаза реализуется технической системой) или сбор (если фаза реализуется человеком) – осуществляет отображение источника информации в сигнал. Здесь определяются качественные и количественные характеристики источника, существенные для решения задач потребителя информации, для чего и собирается или воспринимается информация. Совокупность этих характеристик создает образ источника, который фиксируется в виде сигнала на носителе той или иной природы (бумажном, электронном и т.п.).

2. Передача – перенос информации в виде сигнала в пространстве посредством физических сред любой природы. Включается в информационный процесс, если места выполнения других фаз информационного процесса территориально разобщены.

3. Обработка – любое преобразование информации с целью решения определенных функциональных задач (они определяются потребителем информации). Данная фаза может включать хранение информации как перенос ее во времени.

4. Представление (если потребителем информации является человек) или воздействие (если потребителем является техническая система). В первом случае выполняется подготовка информации к виду, удобному для потребителя (графики, тексты,

диаграммы, таблицы и т.д.). Во втором случае вырабатываются управляющие воздействия на технические средства.

Понятие информационной безопасности

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако, это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства.

В утратившем силу ФЗ «Об информации, информатизации и защите информации» под **информационной безопасностью** понималось *состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства*.

В других источниках приводятся следующие определения:

Информационная безопасность – это

1) *комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с её доступностью для всех авторизованных пользователей*;

2) *показатель, отражающий статус защищенности информационной системы;*

3) *состояние защищённости информационной среды*;

4) *состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.*

В. И. Ярочкин считает, что **информационная безопасность** есть *состояние защищённости информационных ресурсов, технологии их формирования и использования, а также прав субъектов информационной деятельности*.

Достаточно полное определение дают В. Бетелин и В. Галатенко, которые полагают, что

> **Информационная безопасность** – *защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры*.

В данном пособии мы будем опираться на приведённое выше определение.

ИБ не сводится исключительно к защите информации и компьютерной безопасности. Следует различать информационную безопасность от защиты информации.

> **Защита информации** – *деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.*

Иногда под защитой информации понимается создание в ЭВМ и вычислительных системах организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации.

> *Международный день защиты информации отмечается 30 ноября с 1988 года. В этот год произошла первая массовая компьютерная эпидемия - эпидемия червя Морриса.*

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации.

Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. ИБ зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Поддерживающая инфраструктура имеет

самостоятельную ценность, важность которой переоценить невозможно.

После событий 11 сентября 2001 года в законодательстве США в соответствии с законом «О патриотизме» было определено понятие «критическая инфраструктура», которая понимается как «совокупность физических или виртуальных систем и средств, важных для США в такой мере, что их выход из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации». Понятие критической инфраструктуры охватывает такие ключевые области народного хозяйства и экономики США, как национальная оборона, сельское хозяйство, производство пищевых продуктов, гражданская авиация, морской транспорт, автомобильные дороги и мосты, тоннели, дамбы, трубопроводы, водоснабжение, здравоохранение, службы экстренной помощи, органы государственного управления, военное производство, информационные и телекоммуникационные системы и сети, энергетика, транспорт, банковская и финансовая системы, химическая промышленность, почтовая служба.

В социальном плане информационная безопасность предполагает борьбу с информационным «загрязнением» окружающей среды, использованием информации в противоправных и аморальных целях.

Объектом ИБ будет считаться *информация, затрагивающая государственные, служебные, коммерческие, интеллектуальные и личностные интересы, а также средства и инфраструктура её обработки и передачи.*

Также объектами информационного воздействия и, следовательно, информационной безопасности могут быть общественное или индивидуальное сознание.

Общественное сознание – *совокупность идей, взглядов, представлений, существующих в обществе в данный период, в которых отражается социальная действительность.*

На государственном уровне субъектами ИБ являются органы исполнительной, законодательной и судебной власти. В отдельных ведомствах созданы органы, специально занимающиеся информационной безопасностью.

Субъектами ИБ являются *органы и структуры, которые в той или иной мере занимаются ее обеспечением.*

Кроме этого, субъектами ИБ могут быть:

- граждане и общественные объединения;
- средства массовой информации;
- предприятия и организации независимо от формы собственности.

Интересы субъектов ИБ, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

Доступность – возможность за приемлемое время получить требуемую информационную услугу. Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления: производством, транспортом и т.п. Поэтому, не противопоставляя доступность остальным аспектам, доступность является важнейшим элементом ИБ.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Пример области применения средств контроля динамической целостности – анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность – защита от несанкционированного ознакомления. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

Цель мероприятий в области информационной безопасности – защита интересов субъектов ИБ.

Задачи ИБ:

1. Обеспечение права личности и общества на получение информации.

2. Обеспечение объективной информацией.

3. Борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.

4. Защита личности, организации, общества и государства от информационно-психологических угроз.

5. Формирование имиджа, борьба с клеветой, слухами, дезинформацией.

Роль информационной безопасности возрастает при возникновении экстремальной ситуации, когда любое недостоверное сообщение может привести к усугублению обстановки.

Критерий ИБ – гарантированная защищённость информации от утечки, искажения, утраты или иных форм обесценивания. Безопасные информационные технологии должны обладать способностью к недопущению или нейтрализации воздействия как внешних, так и внутренних угроз информации, содержать в себе адекватные методы и способы её защиты.

Информационные опасности и угрозы

Создание системы ИБ предполагает выявление **источников** информационных опасностей и угроз. Существуют **четыре** действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация (искажение), утечка и уничтожение информации. Эти действия являются базовыми для рассмотрения классификации источников информационных опасностей и угроз.

Рассмотрим внешние и внутренние источники информационных опасностей и угроз.

Источниками **внутренних** угроз являются:

1. Сотрудники организации.
2. Программное обеспечение.
3. Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

- ошибки пользователей и системных администраторов;
- нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;
- ошибки в работе программного обеспечения;
- отказы и сбои в работе компьютерного оборудования.

К **внешним** источникам угроз относятся:

1. Компьютерные вирусы и вредоносные программы.
2. Организации и отдельные лица.
3. Стихийные бедствия.

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами или вредоносными программами;
- несанкционированный доступ (НСД) к корпоративной информации;
- информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
- действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;
- аварии, пожары, техногенные катастрофы, стихийные бедствия.

Все перечисленные выше виды угроз (формы проявления) можно разделить на **умышленные** и **неумышленные**. По данным Института защиты компьютеров (CSI), свыше 50% вторжений – дело рук собственных сотрудников компаний. Что касается частоты вторжений, то 21% опрошенных указали, что они испытали рецидивы «нападений». Несанкционированное изменение данных было наиболее частой формой нападения и в основном применялось против медицинских и финансовых учреждений. Свыше 50% респондентов рассматривают конкурентов как вероятный источник «нападений». Наибольшее значение респонденты придают фактам подслушивания, проникновения в информационные системы и «нападениям», в которых «злоумышленники» фальсифицируют обратный адрес, чтобы перенацелить

поиски на непричастных лиц. Такими злоумышленниками наиболее часто являются обиженные служащие и конкуренты.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические, радиоэлектронные и организационно-правовые.

К **информационным** угрозам относятся:

- несанкционированный доступ к информационным ресурсам;
- незаконное копирование данных в информационных системах;
- хищение информации из библиотек, архивов, банков и баз данных;
- нарушение технологии обработки информации;
- противозаконный сбор и использование информации;
-использование информационного оружия.

К **программным** угрозам относятся:

- использование ошибок и «дыр» в программном обеспечении;
- компьютерные вирусы и вредоносные программы;
- установка «закладных» устройств.

К **физическим** угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;
- хищение носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты данных;
- воздействие на персонал.

К **радиоэлектронным** угрозам относятся:

- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К **организационно-правовым** угрозам относятся:

- нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере;
- закупки несовершенных или устаревших информационных технологий и средств информатизации.

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.*

Для защиты интересов субъектов информационных отношений необходимо сочетать **меры** следующих уровней:

1) **законодательный уровень** (законы, нормативные акты, стандарты и т.п.). Законодательный уровень является важнейшим для обеспечения информационной безопасности. К мерам этого уровня относится регламентация законом и нормативными актами действий с информацией и оборудованием, и наступление ответственности нарушение правильности таких действий. Подробнее этот вопрос рассматривается в других главах.

2) **административный уровень** (действия общего характера, предпринимаемые руководством организации). Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

3) **процедурный уровень** (конкретные меры безопасности, ориентированные на людей).

Меры данного уровня включают в себя:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала, обслуживающего систему;
- организацию охраны и режима допуска к системе;

- организацию учета, хранения, использования и уничтожения документов и носителей информации;

- распределение реквизитов разграничения доступа;

- организацию явного и скрытого контроля за работой пользователей;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения.

4) **программно-технический уровень** (технические меры).

Меры защиты этого уровня основаны на использовании специальных программ и аппаратуры и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты:

- идентификацию и аутентификацию пользователей;

- разграничение доступа к ресурсам;

- регистрацию событий;

- криптографические преобразования;

- проверку целостности системы;

- проверку отсутствия вредоносных программ;

- программную защиту передаваемой информации и каналов связи;

- защиту системы от наличия и появления нежелательной информации;

- создание физических препятствий на путях проникновения нарушителей;

- мониторинг и сигнализацию соблюдения правильности работы системы;

- создание резервных копий ценной информации.

Принципы обеспечения информационной безопасности

Организация информационной безопасности предполагает разработку определённых **принципов** её обеспечения. Одним из основных является принцип **баланса интересов личности, общества и государства.** Личность заинтересована в конфиденциальности информации об интимной жизни, доходах, социально значимых ошибках и т.д., а общество заинтересовано в получении сведений об антисоциальных проявлениях, коррупции, преступных доходах и т.д.

Принцип **законности и правой обеспеченности**. Рост значимости ИБ явно опережает развитие соответствующей сферы права, чем умело пользуются и политики, и преступники. Средства массовой информации (СМИ) не несут практически никакой ответственности за ложную информацию, направленную на массового потребителя этой информации (читателя, телезрителя).

Принцип **интеграции с международными системами безопасности информации**. Глобализация жизни на планете требует развития международных коммуникаций и их согласованности в обеспечении безопасности передачи информации.

> **Глобализация** – *процесс всемирной экономической, политической и культурной интеграции и унификации.*

Принцип **экономической эффективности.** Этот принцип говорит о том, что результаты от мер ИБ должны превышать совокупные затраты на них. Если этот принцип не соблюдается, то меры по обеспечению секретности информации не только не окупаются, но даже вредят прогрессу.

Принцип **мобильности системы ИБ**. Система ИБ должна не допускать неоправданных режимных ограничений, т.к. одновременно с этим государство утрачивает возможность защищать главное богатство своей страны – способность создавать и генерировать новые знания.

Принцип **презумпции несекретности информации** означает, что строгому нормированию подлежит конфиденциальность, а не гласность.

При разработке и проведении в жизнь политики информационной безопасности в какой-либо организации целесообразно руководствоваться следующими принципами:

- Принцип **невозможности миновать защитные средства** говорит сам за себя и не требует дополнительных пояснений.

- Принцип **усиления самого слабого звена.** Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения ИБ приобретает нетехнический характер.

- Принцип **невозможности перехода в небезопасное состояние** означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

- Принцип **минимизации привилегий** предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа – уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

- Принцип **разделения обязанностей** предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников.

- Принцип **эшелонированности обороны** предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

- Принцип **разнообразия защитных средств** рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

- Принцип **простоты и управляемости информационной системы.** Залогом информационной безопасности являются не сложность и скрытность, а, напротив, простота и апробированность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование.

- Принцип **обеспечения всеобщей поддержки мер безопасности** носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную

безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

1.2. Окружающая среда как источник информации

Восприятие информации человеком. Особенности восприятия окружающей среды человеком. Перенасыщенная информацией среда. Энергоинформационные свойства воды.

Основные термины и понятия:
Видеоэкология
Вкус
Зрение
Обоняние
Осязание
Слух
Структурная память воды
Шумовое загрязнение

Восприятие информации человеком

Анализаторы являются специальными структурами организма, служащими для ввода внешней информации в мозг для последующей ее переработки. Человек связан со средой с помощью анализаторов, которые состоят из рецепторов, проводящих нервных путей и мозгового конца в коре головного мозга. Мозговой конец состоит из ядра и рассеянных по коре головного мозга элементов, обеспечивающих нервные связи между отдельными анализаторами. Например, когда человек ест, то он чувствует вкус, запах пищи и ощущает её температуру. Основная характеристика анализаторов – чувствительность.

У человека рецепторы настроены на следующие раздражители:

- электромагнитные колебания светового диапазона - фоторецепторы в сетчатке глаза;

- изменение положения тела относительно вектора гравитации - рецепторы вестибулярного аппарата;

- механические колебания воздуха - фонорецепторы уха;

- изменение гидростатического и осмотического давления крови - баро- и осморецепторы;

- воздействие химических веществ – хеморецепторы;

- температурные изменения как внутри организма, так и в окружающей среде – терморецепторы;

Кроме перечисленных, у человека также есть тактильные и болевые рецепторы.

В ответ на изменение условий окружающей среды, чтобы внешние раздражители не вызывали повреждений и гибели организма, в нём формируются компенсаторные реакции, которые могут быть: поведенческими (изменение места пребывания, отдёргивание руки от горячего или холодного) или внутренними (изменение механизма терморегуляции в ответ на изменение параметров микроклимата).

Человек обладает рядом важных специализированных периферических образований – органами чувств, обеспечивающими восприятие воздействующих на организм внешних раздражителей. К ним относятся органы зрения, слуха, обоняния, вкуса, осязания. Нельзя путать понятия «органы чувств» и «рецептор». Например, глаз – это орган зрения, а сетчатка – фоторецептор, один из компонентов органа зрения. Органы чувств сами по себе не могут обеспечить ощущение. Для возникновения субъективного ощущения необходимо, чтобы возбуждение, возникшее в рецепторах, поступило в соответствующий отдел коры больших полушарий.

Рассмотрим отдельные пути поступления информации в организм человека и определим их относительное значение для восприятия целого окружающего пространства.

Зрение является ведущим источником информации для человека. Некоторые исследователи считают, что 90% информации об окружающей среде человек получает с помощью зрения. Мы знаем, как трудно ориентироваться в условиях абсолютной темноты. Зрительный анализатор включает в себя глаз, зрительный нерв, зрительный центр в затылочной части коры головного мозга. Глаз чувствителен к видимому диапазону спектра электромагнитных волн от 0,38 до 0,77 мкм.

Визуальная среда, с которой человек соприкасается каждый день, влияет на орган зрения человека, оказывая воздействие и на

его самочувствие. Неблагоприятная визуальная среда может вызывать у человека раздражение, приводить к тяжелым психическим расстройствам. Изучением окружающей видимой среды как экологического фактора занимается **видеоэкология.**

Большое значение в восприятии человеком окружающей среды имеет **осязание.** Осязание – сложное ощущение, возникающее при раздражении рецепторов кожи, наружных частей слизистых оболочек и мышечно-суставного аппарата. Кожный анализатор воспринимает внешние механические, температурные, химические и другие раздражители кожи. Осязание дополняет зрение в том смысле, что дает информацию об изменении осязательных аспектов окружающей среды. Путем исследований доказано, что человек может жить, потеряв зрение, но без осязания, точки которого рассеяны по всей поверхности тела, он жить не может.

Мы постоянно соприкасаемся с чем-то: с одеждой, с предметами, с которыми работаем. Осязание непосредственно позволяет чувствовать сопротивление и давление и почти не зависит от нашего воображения, чего нельзя сказать о других рецепторах. Таким образом, осязание постоянно информирует нас об особенностях окружающей среды. Материалы нас либо привлекают, либо отталкивают: мы не станем гладить забор из гофрированной жести – этого любимого сегодня строительного материала. Но мы с удовольствием прикоснемся к отполированной годами скамейке у деревенского забора, которая как бы зовет нас к отдыху и размышлениям.

Слух является пассивным органом в процессе восприятия. Слух – способность организма принимать и различать звуковые колебания слуховым анализатором в диапазоне от 16 до 20000 Гц. Порог болевых ощущений 130 – 140 дБ. Человек может закрыть глаза и тем самым исключить восприятие чего-то неприятного, но в ушах у нет никакого клапана. Слух часто дает нам информацию о среде, которая находится вне нашего зрительного поля, за горизонтом, охватываемым зрением. Восприятие пространства в значительной мере зависит от функции слухового аппарата, регистрирующего приятные и неприятные звуки, например шум, который относится к типу невротического влияния окружающей среды – это типичный продукт технически развитого общества.

Шумовое загрязнение – *форма физического (обычно антропогенного) загрязнения, возникающего в результате увеличения интенсивности и повторяемости шума сверх природного уровня. Приводит к повышению утомляемости человека, снижению умственной активности и при достижении 90–100 дБ к постепенной потере слуха.*

Обоняние – способность воспринимать запахи. Животные обладают прекрасным обонянием. Человек обладает разной степенью обоняния к различным пахучим веществам. Приятные запахи улучшают самочувствие человека, а неприятные действуют угнетающе, вызывают отрицательные реакции вплоть до тошноты, рвоты, обморока (сероводород, бензин), способны изменять температуру кожи, вызывать отвращение к пище, приводить к подавленности и раздражительности. В развитии ориентации у ребёнка обоняние играет весьма существенную роль с первых дней жизни. Грудной ребёнок, которому всего несколько дней, может четко различать одежду матери, при этом он руководствуется только обонянием.

В городской среде у человека систематически и подсознательно уменьшается чувствительность органа обоняния. Воздух здесь наполнен таким количеством отработанных газов, что людям ничего не остается, как только постепенно привыкать к ним. Современный человек проявляет все большую склонность к пренебрежению обонянием, хотя именно оно является крайне важной способностью. Пригодность среды для выполнения определенной деятельности человек оценивает, как правило, носом, который по запахам получает информацию там, где глаз не видит, и откуда не доносятся акустические сигналы. Например, легкое ощущение знакомого запаха может вызвать четкие воспоминания о чем-то давно минувшем, например в памяти всплывает живое представление определенной ситуации.

Вкус – ощущение, возникающее при воздействии определённых химических веществ, растворимых в воде, на вкусовые рецепторы, расположенные на различных участках языка. Вкус складывается из четырёх простых вкусовых ощущений: кислое, солёное, сладкое и горькое. Все остальные вариации вкуса – это

комбинации из основных ощущений. Различные участки языка имеют разную чувствительность к вкусовым веществам.

Восприятие окружающей среды происходит путем одновременного взаимодействия всех органов чувств, хотя человек все более становится рабом зрения. Это усиленно закрепляет сегодня аудиовизуальный характер культуры, где на первом месте стоит телевидение. Можно смело утверждать, что современный человек в своей оценке окружающей среды все больше полагается на зрение. Об этом свидетельствует и тот факт, что определенное пространство и возможность его использования для практической деятельности ограничиваются прежде всего визуально.

Есть ли у человека наряду с классическими пятью органами чувств и наряду с чувством, информирующим его о внутренних процессах, происходящих в организме (например, чувство равновесия), другие органы, с помощью которых он может ориентироваться в жизненной среде и получать информацию? В 1976 г. английский психолог Робин Бейкер решил провести исследование скрытых, по его мнению, способностей человека ориентироваться в незнакомой среде, где к тому же отсутствуют важные элементы, облегчающие ориентацию. В этом эксперименте приняли участие 64 студента-зоолога из университета в Манчестере. Им завязали глаза темной материей и посадили в автобус. Затем автобус отправился по очень сложному маршруту, чтобы никто не мог запомнить направление его движения. Проехав 50 км, автобус остановился, и студенты вышли с завязанными глазами. Их задачей было ответить на вопрос: в каком направлении расположен университет? Затем они должны были определить сторону света. Только после этого с них сняли повязку и попросили показать, на этот раз с открытыми глазами, где находится университет.

Согласно результатам исследования, определение направления, сторон света было более правильным, когда они отвечали с повязкой на глазах. Когда у студентов сняли повязку, то точность ответа исчезла. Таким образом, подтверждена была гипотеза, согласно которой человек также обладает органом, воспринимающим действие магнитного поля, в данном случае в ориентировании в незнакомой местности и в определении направления исходной точки.

Особенности восприятия окружающей среды человеком

Человек через доступные ему каналы получает зрительную, звуковую, осязательную, вкусовую информацию и запах. Какими бы физическими характеристиками окружающая среда ни обладала, она всегда воздействует на человека как целое, из чего следует, что импульсы, которые воспринимает человек, никогда не бывают изолированными. Однако он воспринимает не всю поступающую к нему информацию. Он слышит или видит не все звуки и не все световые сигналы, а только те, которые имеют для него определенное значение. При этом на отбор информации влияние оказывают не только физические возможности органов чувств воспринимать информацию, но и такие личностные особенности человека, как отношение к происходящему, его предыдущий опыт, его система ценностей, настроение и т.п., т.е. информация как бы проходит через определенный фильтр. Отбор позволяет отбросить неважную или ненужную информацию. Например, человек может не слышать разговор людей, стоящих рядом, в том случае, если он его не интересует. В то же время отбор информации может привести к потере важной информации, к существенному искажению реальности.

Каждая среда содержит больше информации, чем мы можем сознательно воспринять, зарегистрировать. Наряду с осознанным существует и подсознательное восприятие. Мы получаем информацию, даже не сознавая этого. Такой вид восприятия называется сублимированным. Его существование подтверждено целым рядом экспериментов, среди которых достаточно привести пример подсознательно действующей рекламы.

М. Черноушек указывает на семь видов информации, которые характеризуют ситуации восприятия окружающей среды как целого:

- среда не имеет определенных, твердо фиксированных рамок во времени и пространстве;
- среда воздействует на все чувства, и информацию о среде мы получаем из сочетания данных всех органов;
- среда дает не только главную, но и периферийную информацию;
- любая среда наряду с физическими и химическими особенностями обладает психологическими и символическими значениями;

- среда содержит всегда больше информации, чем мы способны сознательно зарегистрировать и понять;

- среда воспринимается в тесной связи с практической деятельностью, восприятие связано с действием и наоборот;

- окружающая среда воздействует как единое целое.

В результате исследований психологи пришли к выводу, что восприятие ребёнка и взрослого принципиально отличается. Взрослые способны одновременно воспринимать запахи, звуки, зрительную и тактильную информацию. При этом мозг взрослого человека способен эту информацию суммировать и, например, недостаток звуковой информации восполнять зрительной. У детей младше 8 лет восприятие устроено иначе. Мозг ребёнка способен в один и тот же момент обрабатывать информацию только от одного органа чувств: ребёнок либо осязает, либо видит. Суммировать информацию от разных органов чувств человек учится постепенно.

Перенасыщенная информацией среда

Ускоренное развитие техники способствовало тому, что город стал многолюден, перегружен машинами, перенасыщен шумом, визуальными импульсами, другими источниками информации. Современный житель большого города подвергается чрезмерному воздействию информации и его способность воспринимать и интерпретировать сигналы, отличать полезную информацию от ненужной определенным образом изменяется. Он защищается от некоторых импульсов, чтобы воспринимать только те, в соответствии с которыми будет ориентироваться и принимать решения. Таким образом, среда предъявляет все большие требования к личности. И если мы стараемся на шумной главной улице не воспринимать все раздражители, то воздействия некоторых из них мы избежать не можем. Всевозрастающий уровень раздражителей требует новой адаптационной стратегии, заставляет индивида использовать такие источники, которые дают упрощенную информацию. Проблемы и сложности возникают в том случае, когда изменение адаптационного поведения оборачивается потерей существенных данных среды.

Если количество информации превышает средний уровень, то поведение человека может стать слишком простым, рутинным.

Понятие «перенасыщенная среда» впервые применил социолог Г. Зиммель, который уже в начале XX столетия сделал вывод, что городская среда препятствует нормальному отношению людей к новым импульсам, поскольку их энергия распыляется на решение мелких, частных проблем среды. Следовательно, богатая импульсами среда города настолько загружает нас информацией, что остается очень мало времени для восприятия новой информации. Это подтверждает и личный опыт: иногда мы даже не регистрируем изменения в слишком знакомой среде.

Американский психолог Д. Д. Миллер считает, что люди в противодействие перенасыщенной среде вырабатывают специфическую адаптационную стратегию. Они устраняют импульсы, не воспринимают и не концентрируют внимания на информации, которую они не считают для себя важной. Это может себя не оправдать, т.к. мы можем включить во второстепенный ряд и весьма важную информацию. Но часто у людей вообще не остаётся времени для оценки той или иной информации. Мы постоянно спешим, и в спешке действительно невозможно уделить должное внимание импульсам окружающей среды.

Общепризнано ослабление межчеловеческих связей и взаимной социальной ответственности, поскольку в настоящее время человеческая деятельность определяется индивидуальным стремлением к преодолению трудностей перенасыщенной среды. Социально и физически перенасыщенная среда вызывает отчуждение между людьми, ослабляет межчеловеческую солидарность, желание помочь друг другу. Дружеские межчеловеческие отношения в перенасыщенной среде исчезают, особенно по отношению к неизвестным людям.

Энергоинформационные свойства воды

Вода – это самое распространённое вещество на Земле в её приповерхностном слое. Только вода встречается в земных условиях во всех трёх состояниях: твёрдом, жидком и газообразном. С древнейших времён человечество приписывает чудесные свойства воде. При этом большинство её свойств не вписывается в общие физические принципы. Можно утверждать, что вода

– это неизученное вещество. Только в последние годы вода стала подвергаться серьёзному научному изучению.

С. В. Зенин, доктор биологических наук, заведующий проблемной лабораторией Министерства здравоохранения РФ, в результате исследований пришел к выводу, что вода имеет особую молекулярную структуру. Эта структура меняется, если на воду воздействовать различными способами: химическим, электромагнитным, механическим, информационным и т.д. Под этими воздействиями её молекулы способны перестраиваться и таким образом запоминать любую информацию. Феномен «структурной памяти» позволяет воде впитывать в себя, хранить и обмениваться с окружающей средой данными, которые несут свет, мысль, музыка, молитвы или простое слово. Подобно тому, как каждая живая клетка хранит в себе сведения обо всём организме, каждая ячейка воды способна хранить в себе информацию обо всех изменениях в нашей планетарной системе.

Воздействуем ли мы через водную среду друг на друга своими мыслями, словами? Способны ли мы программировать сами себя и окружающих? Безусловно. Способность воды обрабатывать информацию делает её очень похожей на обычный компьютер. Таким образом, человек, состоящий на 70-80% из воды, представляет собой программируемую систему: любые внешние факторы, в том числе и общение людей друг с другом, меняют структуру и биохимический состав жидких сред организма. Это происходит на клеточном уровне, программируется даже сама молекула ДНК, вплоть до полного ее разрушения. Это означает, что нарушения в индивидуальной программе, заложенной в любом организме на молекулярном уровне в воде – это и есть истинная причина и источник болезней, которые проявятся в будущем. Такие ощущения, как резкая усталость, беспричинная агрессия, дурное настроение и даже многие болезни могут стать последствиями негативного энергоинформационного воздействия. И наоборот, чистотой собственных мыслей человек способен поправить собственное здоровье и очистить окружающую среду.

В лаборатории С. В. Зенина исследовали воздействие людей на свойства воды. Контроль велся как по изменению физических параметров, в первую очередь по изменению электропроводности воды, так и с помощью тестовых микроорганизмов.

Исследования показали, что чувствительность информационной системы воды оказалась настолько высокой, что она способна ощущать влияние не только тех или иных полевых воздействий, но и форм окружающих предметов, воздействия человеческих эмоций и мыслей. Вода реагирует на мысли и эмоции окружающих её людей, на события, происходящие с населением и так далее. Кристаллы, образовавшиеся из только что полученной дистиллированной воды, имеют простую форму хорошо известных шестиугольных снежинок. Накопление информации меняет их строение, усложняя и делая их красивее, если информация положительная, и, напротив, искажая или даже разрушая первоначальные формы, если информация отрицательная.

Исследования японского ученого Э. Масару, который замораживал капельки воды, а затем изучал их под сильным увеличением в микроскопе, имеющим встроенную фотокамеру, наглядно подтверждают результаты работы С. В. Зенина. Э. Масару обнаружил, что загрязненная вода имела нарушенную и случайным образом сформированную структуру, а вода из горных потоков и ключей была прекрасно сформирована геометрически.

Далее ученый решил посмотреть, какой эффект оказывает музыка на структуру воды. Он поставил дистиллированную воду между двух колонок на несколько часов и потом сфотографировал её после замораживания. Так же он использовал слова, напечатанные на бумаге и наклеенные на ночь на стеклянную посуду с водой. Полученные фотографии доказывают невероятные изменения воды, как живой субстанции, реагирующей на каждую нашу эмоцию или мысль. Совершенно ясно, что вода легко меняется под воздействием вибраций энергии, независимо от того, загрязненная это или чистая среда. Работа Э. Масару наглядно продемонстрировала различие в молекулярной структуре воды при её взаимодействии с окружающей средой. Этот метод дал возможность показать, каким образом мысли и слова человека воздействуют на его молекулярную структуру.

По мнению С. В. Зенина, вода выступает не просто как жидкость, а как вещество, находящееся в информационно-фазовом состоянии. Вода хранит в себе полную информацию о любых воздействиях на неё. Смысл информационно-фазового состояния воды заключается в том, что полная информация, поступающая в водную среду, отражается в каждой ячейке. В

дополнение к механической, бактериологической и химической очистке воды уже пора всерьёз говорить об информационной очистке и последующим обогащением воды полезной информацией.

1.3. Роль информации в развитии общества

Информационные революции. Информационное общество. Проблема информационного неравенства. Россия в информационной эпохе.

Основные термины и понятия:
Информационная революция
Информационная технология
Информационное неравенство
Информационное общество
Ноосфера
Технологическая революция

Информационные революции

Ряд современных исследователей процесса цивилизационного развития человеческого общества считают, что история человечества может рассматриваться как закономерная последовательность технологических революций.

> **Технологическая революция** − *радикальное изменение доминирующего в обществе технологического уклада, который, в свою очередь, определяется средствами и способами организации общественного производства и жизнеобеспечения общества.*

Профессор А. И. Ракитов показал, что в основе каждой технологической революции лежит информационная революция.

> **Информационная революция** – *это преобразование общественных отношений из-за кардинальных изменений в сфере обработки информации.*

Следствием преобразований общественных отношений является приобретение человеческим обществом нового качества, переход на новый уровень технологического развития.

В настоящее время принято выделять шесть основных информационных революций.

Первая информационная революция (устная) заключается в появлении языка и членораздельной человеческой речи. Развитие языка оказало колоссальное влияние на развитие сознания людей. Язык сделал возможным развитие процессов абстрактного мышления, т. е. зарождения интеллектуальной деятельности людей. В первобытном обществе, когда выживало более организованное племя, возникла необходимость приобретения, сохранения и передачи знаний и умений. В то время использовались и распространялись только «живые знания», носителями которых являлись живые люди − старейшины, жрецы, шаманы. К пожилым людям, имеющим ценный для племени опыт, применялся принцип «не убий». Так возникла система «Учитель» (по Н. Н. Моисееву), которая способствовала развитию не столько в индивидуальной сфере, сколько в общественной.

В условиях первобытного общества процессы накопления знаний и их распространения осуществлялись чрезвычайно медленно, а сохранение уже накопленных знаний в виде легенд, мифов и сказаний было недостаточно надёжным.

Вторая революция (письменная) связана с изобретением письменности. Люди научились отчуждать знания и фиксировать их на материальных носителях в виде рисунков или условных знаков. Это изобретение позволило не только обеспечить сохранность уже накопленных человеческим обществом знаний, но и создать условия для их широкого распространения. Существенным образом изменилась и информационная среда общества, стали возможными новые виды информационных коммуникаций между людьми посредством обмена письменными сообщениями. Позже появились исторические летописи, поэзия и литература, зародились элементы того нового и своеобразного явления, которое мы сегодня называем информационной культурой. Понятие «образование» приобрело новый смысл. Теперь образованным мог считаться только тот человек, который достаточно хорошо владел навыками чтения и письма, причем не только на своём родном языке, но и на других языках.

Третья информационная революция (печатная) началась в эпоху Возрождения (середина XVI в.) и была вызвана изобретением печатного станка. Книгопечатание радикально изменило

общество, культуру, организацию деятельности человека. Относительная простота процесса книгопечатания, большие тиражи печатных книг и их значительно меньшая стоимость по сравнению с рукописными книгами привели к первому информационному взрыву. Произошел взрывообразный рост количества используемых в обществе документов, началось более широкое распространение информации, научных знаний. Появились первые библиотеки печатных книг. Возникла возможность обеспечить сохранение авторства, интеллектуальной собственности (выходные данные книги).

Своего апогея третья информационная революция достигла с появлением печатных СМИ: газет, журналов, рекламных объявлений, информационных справочников и т.п. Несмотря на появление в последние годы различного рода электронных носителей информации, объёмы печатной продукции продолжают расти.

Четвертая информационная революция (электронная) началась в XIX веке и была обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, телевидение. Новые качества, которые принесла в информационную сферу общества эта информационная революция, заключаются не только в том, что по новым коммуникационным сетям стали передаваться невиданные ранее объёмы информации, но также и в том, что информационные коммуникации стали осуществляться с более высокой скоростью. Любое событие, которое происходит сегодня на нашей планете, в течение нескольких часов может стать известным подавляющему большинству её обитателей, где бы они ни находились.

Пятая информационная революция (компьютерная) началась в 50-е годы XX века с появлением средств цифровой вычислительной техники. Применение этих средств для обработки информации кардинальным образом изменило возможности человека по активизации и эффективному использованию информационных ресурсов: роль систематизации, хранения, переработки информации, а также передачи её на расстояние взяла на себя техника. Изобретение в 70-х годах прошлого века микропроцессорной технологии сделало компьютеры доступными для повседневного персонального использования, что во многом изменило психологию и практику научной, педагогической и производственной деятельности людей.

Шестой информационной революцией (сетевой) стало объединение компьютеров для передачи данных в сети, что привело к появлению единого глобального информационного пространства. Некоторые специалисты ставят появление Интернета по его влиянию на цивилизацию в один ряд с книгопечатанием. Интернет – открытая, саморазвивающаяся кибернетическая система, включающая в себя миллионы компьютеров, объединённых в различные локальные и глобальные сети. Использование информационных ресурсов Интернета в образовательных целях ставит ряд философских, психолого-педагогических и методических проблем.

Последняя революция знаменует возникновение безбумажного, виртуального этапа в развитии социальных коммуникаций. Бумага стала необходима только для итогового воспроизводства визуально подготовленных документов. Возникла новая отрасль – **информационная индустрия**, связанная с производством технических средств, методов, технологий для производства новых знаний.

Важнейшими составляющими информационной индустрии становятся все виды информационных технологий, особенно телекоммуникации. При применении информационных технологий достигается экономия затрат труда, энергии людских и материальных ресурсов, необходимых для реализации данного процесса.

> **Информационная технология** – *это представленное в пригодном для практического использования виде концентрированное выражение научных знаний и практического опыта, позволяющее рациональным образом организовать тот или иной достаточно часто повторяющийся информационный процесс*.

Современная информационная технология опирается на достижения в области компьютерной техники и средств связи. Однако с другой стороны, изменения, происходящие в обществе под влиянием сетевых средств массовой коммуникации, не ограничиваются только определенными преимуществами и выгодами, что открывает самые широкие возможности для ведения информационного противоборства в социально-политической

сфере. Информационный терроризм, распространение нелегальных материалов (в том числе безнравственной, возбуждающей низменные человеческие чувства), образование в Сети неформальных молодежных объединений, деструктивное влияние новых коммуникационных технологий на личность − это «оборотная» сторона существования сетевых средств массовой коммуникации.

По расчетам, приведенным Л. Д. Рейманом, пятьдесят лет тому назад, пересылка по почте 30 страниц текста на расстояние 5 тысяч километров длилась бы примерно 10 дней и стоила бы около 30 долларов. Двадцать лет назад, используя факс, подобная пересылка заняла бы примерно 1 час, и стоимость составляла около 50 долларов. Сегодня на это требуется не более 3 секунд, а стоимость составит около 3 центов. Таким образом, стоимость упала в 1000 раз, скорость возросла в 300 тысяч раз.

Бурное развитие компьютерной техники и информационных технологий послужило толчком к развитию общества, построенного на использовании различной информации и получившего название информационного общества.

Информационное общество

По подсчётам ученых, с начала нашей эры для удвоения знаний потребовалось 1750 лет, второе удвоение произошло в 1900 году, третье − в 1950 году и так далее в геометрической прогрессии. Быстрое сокращение времени удвоения объёма накопленных научных знаний указывает на явление, получившее название «информационный взрыв» и свидетельствующее о начале века информации, возникновении информационного общества.

Информационное общество – *это ступень развития цивилизации, в которой главными продуктами производства являются информация и знания.*

В мире активное обсуждение теоретических вопросов развития информационного (постиндустриального) общества

проходило в конце 1970-х – начале 1980-х годов. Концепция информационного общества как общесоциологическая теория развития достаточно глубоко разработана западными исследователями: Д. Беллом, Дж. Гелбрейтом, Дж. Мартином, И. Масудой, Ф. Полаком, Э. Тоффлером, Ж. Фурастье и др. Именно Ж. Фурастье определил постиндустриальное общество как «цивилизацию услуг». Отечественная наука обратилась к данной проблематике значительно позже. Среди отечественных ученых, внесших значительный вклад в развитие этого направления, необходимо отметить В. М. Глушкова, Н. Н. Моисеева, А. И. Ракитова, А. В. Соколова, А. Д. Урсула и др.

Отличительными **чертами** информационного общества являются:

- увеличение роли информации и знаний в жизни и экономике общества;
- возрастание доли информационных коммуникаций, продуктов и услуг в валовом внутреннем продукте;
- быстрое сокращение времени удвоения объёма накопленных научных знаний;
- превышение материальных затрат на хранение, передачу и переработку информации аналогичных расходов на энергетику;
- превращение информации в ресурс общества наряду с природными ресурсами;
- создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение их потребностей в информационных продуктах и услугах;
- сокращение числа людей, занятых в промышленном производстве и сельском хозяйстве.

Кроме положительных моментов прогнозируются и **опасные тенденции** информационного общества:

- усиливается влияние на общество средств массовой информации;
- информационные технологии могут разрушить частную жизнь людей и организаций;
- существует опасность разрыва между «информационной элитой» (людьми, занимающимися разработкой информационных технологий) и потребителями;

- существует проблема отбора качественной и достоверной информации;

- многим людям будет трудно адаптироваться к среде информационного общества.

Одним из основных **критериев** перехода общества к постиндустриальной и далее к информационной стадии развития может служить процент населения, занятого в сфере услуг:

- если в обществе более 50% населения занято в сфере услуг, наступила *постиндустриальная* фаза его развития;

- если в обществе более 50% населения занято в сфере информационных услуг, общество стало *информационным*.

Наряду с вышеуказанными, существуют и другие критерии информационного общества, в частности:

1) превращение информации в основной товар, или увеличение доли стоимости информации в стоимости товаров (в широком смысле). В соответствии с этим критерием общество может быть названо «информационным», если стоимость информации и интеллектуального труда заметным образом превышает стоимость сырьевых товаров, физического труда и т. д.; престижными и высокооплачиваемыми становятся профессии, связанные с владением, накоплением, оперированием информацией и т. д. Внешними признаками перехода общества в состояние «информационного» могут быть преобладание в экономике высокотехнологичных отраслей, престиж профессий, связанных с владением информацией, высокие цены на информационные услуги, экспорт интеллекта в различных его формах (технологий, специалистов и т. п.).

2) качественные изменения в жизненном мире, связанные с разрастанием значимого для индивидов в их повседневной жизни информационного поля.

К описанию эволюции общества применяются разные подходы. Рассмотрим процесс возникновения и развития информационного общества, используя **ритмо-информациологический подход,** предложенный отечественными учеными В. В. Нечаевым и А. В. Дарьиным.

Эволюция человеческого общества может быть охарактеризована двумя фундаментальными процессами: развитием человека и социально–технологическим развитием общества. **Биологический период** (развитие человека) отражает смену

поколений. С течением времени биологический период практически не изменился и его можно считать как среднестатистический возраст родителей при появлении их первого ребёнка, т. е. 20–25 лет.

Периоды и циклы социально–технологического развития характеризуются сменой социальных формаций, например, прогресс в области используемых технологий. Под **технологическим циклом** понимается не только кардинальные революционные изменения технологии (каменный век, железный век), но и последовательная смена технологий и моделей, выражающаяся, например, в поколениях средств связи, средств передвижения и т.п. Абсолютно точно периодичность социального развития установить невозможно. Однако прослеживается общая тенденция: если 5–7 веков назад период социального развития составлял около 200–300 лет, то к началу XXI века он сократился до 1–2 лет.

До конца XIX века базовой характеристикой социального развития общества был технологический уровень. За один и тот же технологический период происходило несколько циклов смены поколений. Следовательно, информационно–несущими выступали периоды смены технологий, накладываемые на более высокую частоту смены поколений людей.

Совпадение периодов биологического и социального развития пришлось на первую половину XX века. При современном уровне развития человечества на время одного поколения приходится несколько технологических циклов, и текущий технологический уровень характеризует лишь сравнительно небольшой интервал жизни человека. Это означает изменение не только лежащих в основе технологий процессов и деятельности, но и всей сопутствующей системы механизмов и средств такой деятельности. Происходит **смена целевых установок**, ценностных ориентаций, системы знаний.

Таким образом, возникновение информационного общества обусловлено сменой информационной составляющей эволюции цивилизации с социального ритма на биологический. Современное общество, начиная с последней четверти XX века, перешло к информационной эре, а информационно–несущим компонентом, определяющим уровень, качество и характеристику цивилизации, стал сам человек.

В прошлом веке В. И. Вернадский писал о том, что неизбежно наступит время, когда эволюционные процессы на нашей планете будет определять человеческая жизнедеятельность. Определяющим началом при этом будет не стихия естественного развития, а разум человека. Таким образом, биосфера станет **ноосферой**, т.е. сферой господства разума человека. В ноосфере люди должны *принять на себя ответственность* за дальнейший ход эволюции на Земле. В условиях быстрых изменений индивидуальные качества человека приобретают ещё более важное значение, чем раньше.

> **Ноосфера** (от греч. nous – разум и sphaira – шар) – *сфера взаимодействия общества и природы, в границах которой разумная человеческая деятельность становится определяющим фактором развития.*

Указанное В. И. Вернадским время наступило «наполовину». С одной стороны, изменения произошли: человеческая деятельность действительно стала заметно влиять на эволюционные процессы. С другой стороны, изменения произошли так быстро, что человечество, в основной массе даже не успело понять этого и не совершилось самого главного – господства разума человека. Наступил экологический кризис, характеризующийся разрушением многих экосистем, истощением ресурсов и загрязнением планеты.

При переходе к информационному обществу возникает новая индустрия переработки информации на базе компьютерных и телекоммуникационных информационных технологий. Ближе всех на пути к информационному обществу стоят страны с развитой информационной индустрией, к числу которых следует отнести США, Японию, Великобританию, Германию, страны Западной Европы. В ряде публикаций отмечается, что США вступили в постиндустриальный период своего развития в 1956 году, а информационным обществом США стали в 1974 году.

Признавая несомненность достижений США и других стран в области информатизации, необходимо понимать, что определенная доля «информационности» этих стран создана за счёт выноса ряда материальных, нередко экологически вредных, производств в другие страны мира, за счёт так называемого «экологического колониализма».

Проблема информационного неравенства

Анализ основных тенденций развития информатизации общества показывает, что этот процесс создает для развития цивилизации не только новые возможности, но и новые проблемы. Возникающая новая высокоавтоматизированная информационная среда оказывается в различной степени доступной для отдельных людей, организаций, регионов и стран мирового сообщества. При этом то общество, которое способно эффективно использовать возможности новой информационной среды для своего научно-технического и социально-экономического развития, получает **существенные** преимущества перед другими субъектами мирового сообщества, которые при этом вытесняются на обочину современного процесса развития цивилизации. Прогнозы специалистов свидетельствуют о том, что глобальная информатизация общества в XXI веке существенно усилит технологическую и экономическую дифференциацию между передовыми и развивающимися странами. Категория развивающихся стран будет всё быстрее размываться, т.к. многие из них перейдут в категорию отсталых стран.

Складывающаяся ситуация, признаки появления которой можно наблюдать уже сегодня, называется проблемой информационного неравенства. О путях преодоления электронно-цифрового разрыва (информационного неравенства) говорится в Окинавской хартии глобального информационного общества, которая была принята лидерами стран «большой восьмерки» 22 июля 2000 года.

В структуре проблемы информационного неравенства специалисты особо выделяют личностно-социальный аспект, который связан с проблемой социальной адаптации человека в новой, быстро изменяющейся информационной среде. Информационное неравенство можно рассматривать как новую форму социального неравенства людей. Снизить остроту этой проблемы призвана перспективная система образования, которая должна предоставить возможность всем членам общества получать необходимые знания и умения для того, чтобы правильно ориентироваться в новом информационном пространстве и эффективно использовать его возможности.

Россия в информационной эпохе

Некоторые исследователи склоняются к мнению, что информационная эра − исторически выигрышный этап для России. Многие особенности российского менталитета, которые с точки зрения индустриального развития можно было считать недостатками, в информационную эру превращаются в достоинства, в частности, отсутствие жесткой привязки к месту и времени, способность переключаться и быстро осваивать новое, беспокойство о судьбах мира и др.

Вошла ли Россия в фазу «информационного» общества или находится на пути к ней? Если рассматривать критерий превращения информации в основной товар, то Россия частично вошла в указанную стадию. Признаками этого могут служить следующие изменения:

- ускоренное развитие сферы информационных услуг: электронные СМИ, компьютеризация, Интернет; развитие сетей информационных услуг, связанных с функционированием банковской и финансовой систем, рынка ценных бумаг, рынков товаров (реклама), рынка недвижимости (риэлторские конторы); информационные юридические услуги (консультирование, нотариат, адвокатура) и т. д.;

- высокая стоимость многих информационных продуктов и услуг;

- престиж и относительно высокая доходность некоторых профессий, связанных с владением и оперированием информацией (экономисты, юристы, госслужба, PR, реклама, политтехнологи, программисты, журналисты, риэлторы и т. п.);

- заметное возрастание спроса на высшее образование и разрастание сети высших учебных заведений (в том числе платных);

- разрастание сети СМИ и формирование информационных «империй»;

- массированное проникновение информационных политтехнологий в политический процесс; возрастание роли информационного воздействия в политической жизни и протекании политических процессов;

- возрастание роли манипулирования массовым сознанием и поведением в функционировании российского общества в целом.

Однако российское общество не может в полном смысле слова быть названо «информационным обществом» ввиду следующих обстоятельств:

- упадок высокотехнологичных секторов экономики (ВПК, космическая отрасль и т. д.);

- полуколониальный характер экспорта (преобладание экспорта сырья);

- низкая стоимость умственного труда (в т. ч. научного, инженерного, преподавательского);

- инфляция и неуклонная деградация высшего образования, связанная со множеством факторов, в т. ч. устареванием материально-технической базы учебного процесса в вузах, ослаблением преподавательских кадров в условиях кризисного существования, массовым применением молодыми людьми учебы в вузах как средства ухода от призыва в армию и т. д.; получение высшего образования само по себе не дает никаких гарантий престижного и выгодного трудоустройства из-за отсутствия реального рынка труда;

- частичность «интернетизации» с точки зрения территориального и социально-пространственного охвата и специфического характера применения Интернет-ресурсов.

По другому критерию – степени изменения в жизненном мире (информационной среде) российского человека – мы, вероятно, уже в полной мере вошли в состояние «информационного общества». Наиболее очевидные признаки этого вхождения: бум рекламы, PR, информационных предложений и т. п. Это массивное изменение создало ряд новых проблем, с которыми российский человек до 90-х годов прошлого века еще не сталкивался. Многие оказались психологически и социально не готовы к произошедшему информационному взрыву и к тому колоссальному массиву информации, который на них обрушился. Кроме этого, информационная среда стала обладать гораздо большей степенью навязчивости, чем прежде. Особенно ярко это проявляется в случае торговой и политической рекламы. Человек становится все более несвободен от навязываемой ему информации.

1.4. Образование в информационном обществе

Особенности обучения в информационном обществе.
Компетентность педагога в информационном обществе.
Информационная пассивность педагога.

Основные термины и понятия:
Информационная пассивность педагога
Компетентность
Профессиональная компетентность учителя безопасности жизнедеятельности

Особенности обучения в информационном обществе

В обществе, где прошлое плавно перетекает в настоящее и повторяет себя в будущем, самым разумным способом подготовки подрастающего поколения к жизни было вооружение его навыками и умениями прошлого с целью использования их в будущем. Знание приобреталось в семье, религиозных организациях и в процессе обучения ремеслу. Прошлый опыт составлял основу содержания обучения.

Развивающейся промышленности XX в. нужен был человек нового типа. Она требовала таких умений и навыков, каких сама по себе ни семья, ни церковь не в состоянии были обеспечить. Возникла система образования, которая уже самой своей структурой воспроизводила новый мир. Школьник не просто изучал факты, он знакомился с образом жизни, который ему предстояло вести. Центр внимания в образовании начал постепенно смещаться от прошлого к настоящему.

Динамизм современных общественных преобразований создает трудности в преемственности опыта поколений: детям приходится овладевать теми знаниями и специальностями, которые были недоступны их родителям. Поэтому сейчас не может идти речь о прямой передаче профессионального опыта. Молодым людям приходится действовать в условиях, когда старый опыт не только не помогает, но иногда даже мешает.

В сфере образования в настоящее время можно выделить следующие признаки информационного общества:

- расширение источников получения знаний в процессе обучения;

- получение образования в любом возрасте и в любое время;

- месторасположение учебного заведения и место проживания обучаемого не имеют особого значения;

- возможность составления программы обучения в соответствии с индивидуальными потребностями и уровнем развития обучающегося.

К сожалению, традиционное образование, которое получают дети и молодежь, должным образом не отражает тот мир, в котором им приходится жить. Динамика образования человека должна повторять, и, в определенной степени, упреждать динамику появления новых знаний. Как отмечают некоторые исследователи, на подготовку человека к будущим событиям сказывается темп изменения окружающей среды. Чем он стремительнее, тем быстрее ускользает от нас современная окружающая обстановка. Однако чем с большей скоростью водитель движется, тем дальше должен быть отодвинут знак, чтобы водитель успел его прочитать и среагировать. Точно так же и общее ускорение темпа жизни вынуждает нас усилить интерес к будущему. Первоочередная задача образования – преодолеть отставание от запросов современной жизни, а это значит, что в подготовке учеников необходимо учитывать не только проблемы и потребности сегодняшнего дня, но и те, что проявятся **в будущем.**

Современное общество в виду высокой скорости изменений в жизни выдвигает справедливое требование непрерывности образования. Современное среднее образование дает тот минимальный уровень знаний, которым должен обладать каждый член современного общества. Получив высшее образование, современный человек лишь в определенной мере достигает текущего минимально необходимого уровня знаний и технологий в какой-либо области. Далее выпускник вынужден в соответствии с появлением новых знаний повышать свой профессиональный уровень.

Для человека процесс потребления большого количества информации может представлять опасность. Новая информация может не совпадать с прошлым опытом, нормами и ценностями человека. Поэтому постиндустриальный тип общества характеризуется появлением нового вида грамотности – информационной, когда на первый план выдвигаются такие качества, как умение собрать информацию для решения задачи, способность анализировать и обобщать, умение быстро ориентироваться в глобальном информационном пространстве и др.

Компетентность педагога в информационном обществе

Частая смена технологий в современном мире означает трансформацию не только лежащих в её основе процессов и деятельности специалистов, но и всей сопутствующей системы механизмов и средств такой деятельности. Изменения в обществе требуют повышения профессиональной компетентности педагогов, а также коррекции содержания отдельных предметов и стратегии образования в целом. Можно предположить, что ориентация сознания учителя на будущее станет звеном, объединяющим его профессиональную и социальную компетентность.

Компетентность – *специфическая способность, позволяющую человеку конструктивно действовать в изменяющихся социальных и профессиональных условиях.*

Профессиональная компетентность учителя безопасности жизнедеятельности – *соответствующая определенной компетенции способность учителя осуществлять педагогическую деятельность с учетом специфики курса «Основы безопасности жизнедеятельности».*

Образование – социальный институт, формирующий потребности и облик будущего общества. Образование предопределяет личностные качества каждого человека, его знания, умения, навыки, мировоззренческие и поведенческие приоритеты, а, следовательно, в конечном итоге – экономический, интеллектуальный, нравственный и духовный потенциал общества. Необходимо формировать у учителя и у учащихся новое, обращенное в будущее**,** мышление, которое способно решить задачи, как развития цивилизации, так и сохранения окружающей среды.

Среди стереотипов педагогического мышления особо выделяется ориентация на конечность образования, которая понимается как подготовка к жизни, выполнение определенных социальных ролей. На практике этот стереотип приводит к стремлению научить всему и навсегда, усвоению готовых знаний, перегрузке учебных программ конкретным материалом, догматизму и формализму мышления. Преодоление этого стереотипа в условиях лавинообразного возрастания объёмов информации и

её быстрого старения, поддержание удовлетворительной компетенции педагога требует формирования у него новой установки на непрерывное образование и необходимость самообразования.

Преподаватель современной школы обязан не только информационно соответствовать сегодняшнему дню, но и знать направления дальнейшего информационного развития цивилизации с возможными опасностями этого развития. Имеющаяся у рядового педагога информационная картина мира, по большому счёту, не соответствует существующей реальности и препятствует осознанию ответственности человека за происходящие негативные изменения в современном мире. Компетентность современного педагога должна включать в себя мировоззренческую и философскую составляющие. Владея философскими категориями, научным пониманием процесса познания и методами научного познания, педагог будет готов действовать конструктивно в изменяющихся социальных и профессиональных условиях.

Образовательные учреждения находятся внутри достаточно стабильной среды, но их окружает большое число внешних элементов, которые трансформируются. Хотя изменения носят постепенный и предсказуемый характер, педагог должен следить за тем, что происходит в среде, с тем, чтобы своевременно прореагировать на происходящие изменения, а в идеальном случае – предвосхитить их. Адаптируясь, таким образом, к меняющимся потребностям общества, педагог активно влияет на его состояние, предопределяя и сами эти потребности. В условиях распространения информационных и коммуникационных технологий роль учителя как источника информации должна постепенно отойти на второй план, а главными для педагога должны стать **воспитательные** задачи.

Традиционно в общественный образ учителя вкладываются идеальные представления, связанные с его способностью «сеять разумное, доброе, вечное». В российской традиции учитель ассоциируется с духовным наставником, просветителем. Он, прежде всего, творец мировоззрения, а потом уже предметник. В настоящее время формируется иная общественная позиция: учитель – функционер, формальным предназначением которого является передача социального знания. Но учитель-функционер не может подготовить молодых людей к жизни в обществе социальных перемен с его высокими требованиями к

качествам личности. Отсюда всё в большей мере общественные ожидания связывают деятельность учителя с творческой самостоятельностью, поиском, высоким профессионализмом.

Учитель не свободен от условий, в которых он живет и работает. Но он свободен занять ту или иную позицию по отношению к ним. Поэтому, в конечном счёте, не учитель должен быть подвластен условиям, а скорее, условия подвластны ему. Сознательно или бессознательно он решает, будет ли он противостоять неблагоприятным условиям или позволит себе быть управляемым ими.

Информационная пассивность педагога

Информационная пассивность педагога как вид информационного поведения сформировалась ещё в советский период. Низкая социальная значимость информации в обществе вела к отсутствию интереса к ней, что выражалось в информационной пассивности граждан, создавая нездоровую информационную среду, феномен боязни использования и обмена информации. Жесткая регламентация школьной жизни породила исполнительного, равнодушного, лишенного инициативы педагога, сформировала пренебрежительное отношение к новаторскому поиску и опыту. Бюрократическое управление системы образования противилось внедрению в педагогическую практику нового и передового, укрепляя в педагогах состояние беспомощности. Отсутствие привычки к информационной обеспеченности привело к информационной нетребовательности и безразличию.

Информационная пассивность педагога характеризуется:

- несоответствием информационной картины мира педагога существующей реальности и требованиям информационного общества;

- прекращением своего профессионального самообразования и самовоспитания после накопления определенного количества информации и методической базы для преподавания своего предмета;

- нежеланием совершенствования навыков работы с информацией и повышения своей информационной компетентности (информационной культуры);

- неумением отобрать из огромной массы информации, в том числе при помощи компьютера, наиболее ценную и необходимую,

обработать и систематизировать, а также обеспечить хранение, которое гарантирует её сохранность, легкость и экономичность использования.

Согласно результатам исследований, только 44% учителей в возрасте до 30 лет обращаются к дополнительным информационным психолого-педагогическим источникам, у учителей в возрасте 40 лет и старше интерес к таким источникам почти исчезает. Низкий уровень готовности к повышению профессиональной компетентности подтверждаются другими данными: лишь 10-14% педагогов способны критически отнестись к собственному опыту.

Стремительный рост объёма информации тоже создает условия для возникновения информационной пассивности – возникает проблема в отслеживании новой информации даже с учётом узкой профессиональной специализации. У человека становится всё меньше времени для того, чтобы углубиться в изучение какого-либо вопроса. Избыток имеющейся информации в совокупности с неумением работать с большими объёмами информации является такой же преградой для становления профессиональной компетентности, как и отсутствие необходимых условий для её поиска и обработки.

Вопросы для самоконтроля

1. Дайте определение «информации».
2. Почему существует множество определений «информации»?
3. Дайте определение «информационной безопасности».
4. Почему существует множество определений «информационной безопасности»?
5. Перечислите виды информации.
6. Перечислите атрибутивные свойства информации.
7. Перечислите прагматические свойства информации.
8. Перечислите динамические свойства информации.
9. Перечислите фазы, составляющие информационный процесс.
10. Приведите примеры информационных процессов в природе.
11. Приведите примеры информационных процессов в технических системах.

12. Каковы цели и задачи информационной безопасности?

13. Приведите примеры опасностей и угроз в сфере информационных процессов и систем.

14. Назовите источники информационных внешних угроз.

15. В каких формах могут проявляться внутренние угрозы?

16. Назовите источники информационных внутренних угроз.

17. В каких формах могут проявляться внешние угрозы?

18. В чем суть защитных мер законодательного уровня?

19. В чем суть защитных мер административного уровня?

20. В чем суть защитных мер процедурного уровня?

21. В чем суть защитных мер программно-технического уровня?

22. Назовите несколько принципов обеспечения информационной безопасности.

23. Перечислите пути поступления информации в организм человека.

24. Какими информационными свойствами обладает вода?

25. В чём может заключаться информационная очистка воды?

26. Перечислите информационные революции и дайте их краткую характеристику.

27. Покажите на примерах значение информации в развитии общества.

28. Что такое информационное общество? Каковы его отличительные черты?

29. Что такое информационное неравенство людей в информационной среде? Каковы его причины?

30. В чём причины информационной пассивности педагога?

31. Почему в условиях распространения информационных и коммуникационных технологий главными для педагога должны стать воспитательные задачи?

ГЛАВА 2. ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Информация как объект правового регулирования

Информационные правоотношения.
Понятие и виды информации, защищаемой законодательством РФ.

Основные термины и понятия:
Документированная информация
Информационные правоотношения

При рассмотрении информации в качестве предмета правоотношений в правовой системе, приходится возвращаться к определению информации в его исходном смысле: под информацией понимается содержание сообщений, сведений и сигналов. В основе такого подхода (антропоцентрического) к определению понятия «информация» лежит идея, что в процессе создания, распространения, преобразования и потребления информации подавляющее большинство общественных отношений возникает именно по поводу информации в форме сведений или сообщений. Кроме понятия «информация» ФЗ «Об информации, информационных технологиях и о защите информации» вводит термин «документированная информация».

> **Документированная информация** − *зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.*

Информационные правоотношения

Правовое обеспечение защиты информации представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию и функционирование защиты конкретных объектов и систем.

Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включаются:

- законодательство об интеллектуальной собственности;
- законодательство о средствах массовой информации;
- законодательство о формировании информационных ресурсов и предоставлении информации из них;
- законодательство о реализации права на поиск, получение и использование информации;
- законодательство о создании и применении информационных технологий и средств их обеспечения.

В соответствии с действующим законодательством

Информационные правоотношения − *это отношения, возникающие при:*

- формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

- создании и использовании информационных технологий и средств их обеспечения;

- защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

В отрасли права, акты которых включают информационно-правовые нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

Понятие и виды информации, защищаемой законодательством РФ

Статья 5 ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает две группы информационных ресурсов по категориям доступа: открытые информационные ресурсы и информационные ресурсы, доступ к которым ограничен в соответствии с законом.

Все государственные информационные ресурсы РФ являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации» защите подлежат сведения ограниченного доступа, а степень защиты определяет их собственник.

Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Информация с ограниченным доступом, в свою очередь, подразделяется на сведения, составляющие **государственную тайну** и **конфиденциальную информацию.**

Конфиденциальная информация классифицируется следующим образом:

- коммерческая тайна;
- служебная тайна;
- профессиональная тайна;
- персональные данные;
- иные виды тайн.

В Указе Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» утвержден перечень сведений конфиденциального характера, в котором перечислены шесть видов информации:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом (ГК) РФ и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

- содержащая государственную тайну (Закон РФ «О государственной тайне», ст. 275, 276, 283, 284 УК РФ);

- передаваемая путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ, ст. 63 ФЗ «О связи», ст. 138 Уголовного кодекса (УК) РФ); касающаяся тайны усыновления (ст. 139 Семейного кодекса (СК), ст. 155 УК РФ);

- содержащая служебную тайну (ст. 139 ГК РФ), коммерческую тайну (ст. 139 ГК РФ и ст. 183 УК РФ), банковскую тайну (ст. 183 УК РФ), личную тайну (ст. 137 УК РФ), семейную тайну (ст. 137 УК РФ), информация, являющаяся объектом авторских и смежных прав (Закон РФ «Об авторском праве и смежных правах», ст. 146 УК РФ);

- информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (ФЗ «Об информации, информационных технологиях и о защите информации», ст. 140 УК РФ) и др.

Уголовный кодекс РФ вводит нормы, объявляющие общественно опасными деяниями конкретные действия в сфере компьютерной информации и устанавливающие ответственность за их совершение. К преступлениям отнесены неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

В тех случаях, когда общественно опасные действия в области информационных отношений совершаются без применения компьютерных средств, законодатель нередко относит их к другим соответствующим родовым объектам.

Клевета или оскорбление (ст. 129, 130), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140), нарушение авторских, смежных изобретательских и патентных прав (ст. 146, 147), разглашение тайны усыновления (удочерения) (ст. 155) находятся в разделе «Преступления против личности».

Кража, мошенничество, хищение предметов, имеющих особую ценность, умышленное уничтожение или повреждение имущества, заведомо ложная реклама, изготовление и сбыт поддельных кредитных карт, незаконный экспорт технологий, научно-технической информации (ст. 158, 159, 164, 167, 182, 187, 189) – в разделе «Преступления в сфере экономики» и т.д.

2.2. Защита государственной тайны

Государственная тайна как особый вид защищаемой информации. Ущерб от утечки сведений, составляющих государственную тайну. Система защиты государственной тайны. Способы защиты государственной тайны. Режим секретности.

Основные термины и понятия:
Государственная тайна
Защита сведений, составляющих государственную тайну, и их носителей
Сведения особой важности
Сведения секретные
Сведения совершенно секретные

Государственная тайна как особый вид защищаемой информации

В современном мире информация рассматривается как один из наиболее ценных продуктов человеческой жизнедеятельности, а информационные ресурсы и технологии, которыми располагает государство, определяют его стратегический потенциал и влияние в мире. В результате безопасность государства, его общественно-политических институтов, организаций и граждан включает в настоящее время в качестве обязательной составляющей информационную безопасность. Важным элементом информационных ресурсов является государственная тайна, отнесенная по условиям правового режима к документированной информации ограниченного распространения.

Тайны являются неотъемлемой составляющей общественной жизни, частью правовой системы и могут служить даже своеобразным мерилом для определения вида политического режима в государстве, ибо состояние защиты секретов отражает характер взаимоотношений общества и государства, демократизации государственной власти.

Государственные средства воздействия на информационные процессы − важнейшее политическое условие обеспечения прав человека и рационализации использования информационных ресурсов в обществе. Система защиты секретов − наиболее сильное звено государственного опосредования общественных отношений в информационной сфере. Сведения, составляющие государственную тайну, имеют особую важность для общества и государства.

Вследствие величины возможного ущерба от её разглашения государственная тайна занимает приоритетное место в системе социального института тайн. Режим защиты государственной тайны – важнейший элемент системы государственного управления.

Правовой институт государственной тайны − признанный всеми странами институт регулирования информационных общественных отношений. Государственная секретность в той или иной степени наличествует во всех государствах мира. Это вполне объяснимо и логично, поскольку информация, с одной стороны − объект отношений людей, а с другой − ресурс: ре-

сурс управления, принятия решений. Поэтому в качестве реальной угрозы своей безопасности государства рассматривают потенциально возможную утечку защищаемой информации за границу.

Правовой институт государственной тайны имеет три составляющие:

1) сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна);

2) режим секретности (конфиденциальности) − механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты;

3) санкции за неправомерное получение и (или) распространение этих сведений.

Понятие «государственная тайна» является одним из важнейших в системе защиты государственных секретов в любой стране. От её правильного определения зависит и политика руководства страны в области защиты секретов. Определение этого понятия дано в Законе РФ «О государственной тайне».

> **Государственная тайна** − *защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.*

В этом определении указываются категории сведений, которые защищаются государством, и сообщается, что распространение этих сведений может нанести ущерб интересам государственной безопасности. Для сравнения приведем краткие определения понятия «государственная тайна», даваемые специалистами других стран.

В Уголовном кодексе ФРГ зафиксировано, что государственной тайной являются факты, предметы или познания, которые доступны лишь ограниченному кругу лиц и должны содержаться в тайне от иностранного правительства, чтобы предотвратить опасность наступления тяжкого ущерба для внешней безопасности ФРГ.

В Исполнительном Указе Президента США от 2.04.1982 г. говорится, что к информации по национальной безопасности относится определенная информация по национальной обороне и международным вопросам, которая защищается от несанкционированного раскрытия.

В некоторых странах это понятие выражается в других терминах, например, в Японии – «оборонный секрет».

Модель определения государственных секретов обычно включает в себя следующие существенные признаки:

1) предметы, явления, события, области деятельности, составляющие государственную тайну;

2) противник (данный или потенциальный), от которого в основном осуществляется защита государственной тайны;

3) указание в законе, перечне или инструкции сведений, составляющих государственную тайну;

4) наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т.п. в случае разглашения (утечки) сведений, составляющих государственную тайну.

Важным признаком государственной тайны является степень секретности сведений, отнесенных к ней. В нашей стране принята следующая система обозначения сведений, составляющих государственную тайну: «особой важности», «совершенно секретно», «секретно». Эти грифы проставляются на документах или изделиях (их упаковках или сопроводительных документах). Содержащиеся под этими грифами сведения являются государственной тайной.

К сведениям **особой важности** (Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности, указанные в Постановлении Правительства РФ от 4 сентября 1995 г. № 870) следует относить такие сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях.

К **совершенно секретным** сведениям следует относить такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях.

К **секретным** сведениям следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб

может быть нанесен интересам предприятия, учреждения или организации.

Перечень сведений, которые могут быть отнесены к государственной тайне, содержится в ст. 5 Закона РФ «О государственной тайне».

Государственную тайну составляют:

1) **сведения в военной области:**

- о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

- о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

- о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

- о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

- о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

- о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и со-

стоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) **сведения в области экономики, науки и техники:**

- о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

- об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

- о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

- об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанного вооружения, военной техники и другой оборонной продукции;

- о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

- об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) **сведения в области внешней политики и экономики:**

- о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

- о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) **сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:**

- о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

- о методах и средствах защиты секретной информации;

- об организации и о фактическом состоянии защиты государственной тайны;

- о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

В статье 7 Закона РФ «О государственной тайне» приведён перечень сведений, **не подлежащих** отнесению к государст-

венной тайне и засекречиванию. Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Ущерб от утечки сведений, составляющих государственную тайну

Понятие, виды и размер ущерба разработаны пока ещё недостаточно и, видимо, будут различны для каждого конкретного объекта защиты: содержания сведений, составляющих государственную тайну, сущности отраженных в ней фактов, событий, явлений действительности. В зависимости от вида, содержания и размеров ущерба можно выделить группы некоторых видов ущерба при утечке (или возможной утечке) сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т.д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т.д. Экономический ущерб может быть выражен прежде всего в денежном исчислении. Экономи-

ческие потери от утечки информации могут быть прямые и косвенные.

Прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороны страны, которые в результате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку. Косвенные потери чаще всего выражаются в виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате чего соперник быстрее довел свои исследования до завершения и запатентовал их и т.д.

Моральный ущерб, как правило, неимущественного характера, наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны, приведшую к выдворению из каких-то государств наших дипломатов, разведчиков, действовавших под дипломатическим прикрытием, и т.п.

Тенденция увеличения степени открытости государства перед обществом диктует необходимость максимально возможного сокращения числа сведений, относимых к государственной тайне, открытости общего перечня относимых к ней категорий сведений, механизмов засекречивания и условий рассекречивания. Обязанность государства − взять на себя формирование взвешенного механизма защиты различных видов информации и установления рамок действия институтов тайн. Такие требования возникают из потребности современного общества быть более открытым и доступным, и диктуются необходимостью обеспечения безопасности личности, общества и государства.

Система защиты государственной тайны

В общем смысле защита информации − комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих её распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и её носителям.

Защита информации разбивается на решение двух основных групп задач:

1) своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой, инженерно-технической, маркетинговой и иной деятельности, т.е. обеспечение специалистов организаций, предприятий и фирм секретной или конфиденциальной информацией;

2) ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях.

При решении первой группы задач учитывается, что специалисты могут использовать как открытую, так и засекреченную информацию. Снабжение специалистов открытой информацией ничем не ограничивается, кроме её фактического наличия. При снабжении же специалиста засекреченной информацией действуют ограничения: наличие соответствующего допуска (к какой степени секретности информации он допущен) и разрешения на доступ к конкретной информации. В решении проблемы доступа специалиста к соответствующей засекреченной информации всегда существуют противоречия: необходимо, с одной стороны, максимально ограничить его доступ к засекреченной информации и тем самым уменьшить вероятность утечки этой информации, а с другой – наиболее полно удовлетворить его потребности в информации, в том числе и засекреченной, для обоснованного решения им служебных задач.

Вторая группа задач включает в себя такие условия, как:

- защита информационного суверенитета страны и расширение возможностей государства по укреплению своего могущества за счёт формирования и управления развитием своего информационного потенциала;

- обеспечение безопасности защищаемой информации: предотвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмешательства в информацию и информационные системы;

- сохранение секретности информации в соответствии с установленными правилами её защиты, в том числе предупреждение её утечки и несанкционированного доступа к её носителям;

- сохранение полноты, достоверности, целостности информации и её массивов и программ обработки;

- недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству.

Вопросы защиты государственной тайны приобрели особую значимость в последние годы, в период глубоких социально-экономических преобразований в РФ, когда, с одной стороны, появились новые угрозы безопасности государства, а, с другой стороны, сложившиеся режимы защиты государственной тайны перестают срабатывать должным образом.

В ст. 2 Закона РФ «О государственной тайне» дано определение системы защиты государственной тайны.

> **Система защиты государственной тайны** − *совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.*

Система защиты сведений, отнесенных к государственной тайне, и их носителей складывается из:

- органов защиты государственной тайны;
- средств и методов защиты государственной тайны;
- проводимых мероприятий.

> З**ащита сведений, составляющих государственную тайну, и их носителей** – *деятельность органов защиты этой тайны, направленная на обеспечение безопасности информации, отнесенной к государственной тайне, предотвращение её утечки и её максимально эффективное использование.*

Главным субъектом, осуществляющим защиту сведений, составляющих государственную тайну, является государство в лице его высших органов власти и управления, которое располагает всей полнотой властных полномочий по решению задач защиты государственной тайны. В ст. 4 Закона РФ «О государственной тайне» определены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защите. Распоряжением Пре-

зидента РФ от 11 февраля 1994 г. № 73-рп утвержден перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.

Высшие органы государственной власти и управления создают нормативно-правовую базу, регламентирующую деятельность по защите сведений, отнесенных к государственной тайне. Координация деятельности по разработке и выполнению государственных программ, по подготовке нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне, возложена на Межведомственную комиссию. Каждый орган и должностное лицо наделяются полномочиями по проведению организационно-правовых мероприятий по защите государственной тайны (Закон РФ «О государственной тайне», ст. 20).

В систему защиты государственной тайны включаются кроме мер, осуществляемых непосредственно в местах сосредоточения и обращения сведений, составляющих эту тайну, также проводимые государством мероприятия и устанавливаемые административно-правовые режимы:

- борьба со шпионажем и разглашением государственной тайны;
- охрана государственных тайн в печати;
- пограничный режим;
- режим въезда и передвижения иностранцев;
- режим выезда специалистов в служебные командировки за границу.

Они в качестве составных элементов включаются в систему защиты государственной тайны и в большинстве своём играют роль препятствия, преграды в возможных каналах утечки секретной информации.

Рассматривая проблемы деятельности по защите государственной тайны, можно назвать ряд факторов, которые предопределяют её формирование и состояние. Организация деятельности по защите государственных секретов в стране зависит от военно-политической обстановки в мире и стране. Обострение международной обстановки обычно приводит к усилению деятельности спецслужб противоборствующих сторон и соответственно к ужесточению принимаемых мер по защите своих секретов.

Уровень защиты секретной информации в определенной степени должен соответствовать важности этой информации для

собственника и интенсивности действий потенциального противника по добыванию секретов о нашем государстве. Защита секретов должна носить превентивный характер: меры защиты секретной информации должны предупреждать возможность несанкционированного доступа к засекреченной информации и возможные вредные последствия, которые могут наступить в случае утечки секретной информации.

Организация защиты государственной тайны находится в зависимости от принятой системы и критериев засекречивания информации: чем больше засекречивается информации, тем больше требуется сотрудников для её обработки, хранения и выдачи, тем выше стоимость её защиты; чем выше степень секретности информации, тем выше уровень её защиты, и т.д. После засекречивания информация начинает жить своей собственной жизнью: практически уже не имеет значения, произведено засекречивание сведений, действительно составляющих государственную тайну, или информация засекречена «на всякий случай», чтобы что-то скрыть и т.п. Секретная информация сама начинает «диктовать» условия своей защиты режимным службам и другим исполнителям.

Расширение круга засекречиваемых сведений и значительное увеличение в связи с этим количества секретной информации затрудняет её защиту, а увеличение числа лиц, допущенных к этой информации, усиливает вероятность её утечки. А это начинает противоречить одному из основных принципов защиты секретной информации – максимальному ограничению числа лиц, допускаемых к секретам.

Система защиты информации включает в себя совокупность элементов, её образующих, и их свойства. Внутренние связи системы и их свойства составляют архитектуру системы, её структуру и внутреннюю организацию. Одновременно элементы системы имеют внешние связи, которые целенаправленно воздействуют на внешнюю среду и решают поставленные перед системой задачи, это – функциональная часть системы. Вполне естественно, что обе части системы – структурная и функциональная – не отделены друг от друга: это как бы две стороны одних и тех же элементов, составляющих систему защиты информации.

Структурная часть системы защиты информации составляет её внутреннюю организацию, которая позволяет системе нормально функционировать, создает условия для обеспечения безопасности засекреченной информации, её обращения только по каналам, контролируемым данной системой.

Структурная часть системы защиты информации включает:

1) систему законов и других нормативных актов, устанавливающих:

- порядок и правила защиты информации, а также ответственность за покушение на защищаемую информацию или на установленный порядок её защиты;

- защиту прав граждан, связанных по службе со сведениями, отнесенными к охраняемой тайне;

- права и обязанности государственных органов, предприятий и должностных лиц в области защиты информации;

2) систему засекречивания информации, в которую входят:

- законодательное определение категории сведений, которые могут быть отнесены к государственной тайне;

- законодательное и иное правовое определение категорий сведений, которые не могут быть отнесены к государственной тайне;

- наделение полномочиями органов государственной власти и должностных лиц в области отнесения сведений к охраняемой законом тайне;

- составление перечней сведений, отнесенных к государственной тайне;

3) систему режимных служб и служб безопасности с их собственной структурой, штатным расписанием, обеспечивающими функционирование всей системы защиты информации.

Структурная часть системы защиты информации является устойчивой частью данной системы, её консервативной частью. Как видно из перечисления основных элементов структурной части системы, её элементы могут изменяться только «скачкообразно», они не могут приспосабливаться быстро и непрерывно в зависимости от изменения внешней среды, а также изменения обстановки, поскольку внешняя среда может оказывать влияние на структурную часть системы защиты информации лишь через её функциональную часть, т.е. опосредованно.

Функциональная часть системы защиты информации решает задачи обеспечения засекреченной информацией деятельности вышестоящей системы, в которую данная система защиты информации «встроена». В эту деятельность вовлекается широкий круг работников объекта: сотрудники службы безопасности, связанные с обработкой, хранением, выдачей и учётом засекреченной информации; руководители объекта и структурных подразделений; исполнители, т.е. все работники объекта, которые являются потребителями защищаемой информации.

Способы защиты государственной тайны

Основными организационными и техническими способами, используемыми в защите государственной тайны, являются: скрытие, ранжирование, дробление, учёт, дезинформация, морально-нравственные меры, кодирование и шифрование.

Скрытие как метод защиты информации является в основе своей реализацией на практике одного из основных организационных принципов защиты информации – максимального ограничения числа лиц, допускаемых к секретам. Скрытие – один из наиболее общих и широко применяемых методов защиты информации. Реализация этого метода достигается обычно путём:

- засекречивания информации, т.е. отнесения её к секретной или конфиденциальной информации различной степени секретности и ограничения в связи с этим доступа к этой информации в зависимости от её важности для собственника, что проявляется в проставляемом на носителе этой информации грифе секретности;
- устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Ранжирование как метод защиты информации включает, во-первых, деление засекречиваемой информации по степени секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа.

Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

Дезинформация – метод защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности. Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом. Этот способ применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве товаров народного потребления.

Морально-нравственные способы защиты информации можно отнести к группе тех методов, которые, исходя из расхожего выражения, что «тайну хранят не замки, а люди», играют очень важную роль в защите информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапливающий в своей памяти колоссальные объёмы информации, в том числе секретной, нередко становится источником утечки этой информации или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предполагают прежде всего воспитание сотрудника, допущенного к секретам, т.е. проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, осведомленного в сведениях, составляющих охра-

няемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Учёт также является одним из важнейших методов защиты информации, обеспечивающим возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также данные обо всех пользователях этой информации. Без учёта решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объём.

Принципы учёта засекреченной информации:

1) обязательность регистрации всех носителей защищаемой информации;

2) однократность регистрации конкретного носителя такой информации;

3) указание в учётах адреса, где находится в данное время данный носитель засекреченной информации;

4) единоличная ответственность за сохранность каждого носителя защищаемой информации и отражение в учётах пользователя данной информации в настоящее время, а также всех предыдущих пользователей данной информации.

Кодирование – метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что оно может попасть в руки соперника, а также при обработке и хранении информации в средствах вычислительной техники.

Для кодирования используются обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при помощи которых информация может быть преобразована (закодирована) таким образом, что прочесть её можно будет только если потребитель располагает соответствующим ключом (кодом) для её раскодирования. Кодирование информации может производиться с использованием технических средств или вручную.

Шифрование – метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра.

Шифрование может быть предварительным (шифруется текст документа) и линейным (шифруется разговор). Для шифрования информации может использоваться специальная аппаратура.

Знание возможностей приведенных методов позволяет активно и комплексно применять их при рассмотрении и использовании правовых, организационных и инженерно-технических мер защиты секретной информации.

Режим секретности

При рассмотрении проблем защиты информации часто затрагивается вопрос о режиме секретности или конфиденциальности (в дальнейшем – режим секретности). Понятие «режим секретности» тесно связано с понятием «защита информации», переплетается с ним, а иногда и отождествляется.

Режим секретности является частью системы защиты засекреченной информации, а точнее, это реализация системы защиты информации для конкретного объекта или одного из его структурных подразделений или конкретной работы.

Основное назначение режима секретности – обеспечить соответствующий уровень защиты информации, т.к. чем выше степень её секретности, тем более высокий уровень её защиты устанавливается, соответственно изменяется и режим секретности. Режим секретности – это не регламентация правовых норм и правил защиты сведений, а реализация на конкретном объекте действующих норм и правил защиты сведений, составляющих государственную тайну, установленных и регламентированных соответствующими законодательными и подзаконными нормативными актами.

Режим секретности включает следующие группы мер:

- разрешительную систему, определяющую порядок доступа в служебных целях конкретных сотрудников к определен-

ной защищаемой информации и в конкретные помещения, где ведутся конфиденциальные или секретные работы;

- порядок и правила делопроизводства с секретными или конфиденциальными документами и иными носителями защищаемой информации. Возможно разделение потоков документальной информации по степени секретности сведений, содержащихся в документах, а также разделение потоков информации, документов, содержащих государственную и коммерческую тайну;

- установление пропускного и внутри объектового режима, соответствующего степени секретности информации, имеющейся на объекте;

- воспитательно-профилактическую работу, уровень и содержание которой должны соответствовать уровню требуемой защиты информации с целью предотвратить или значительно уменьшить риск утечки засекреченной информации через сотрудников объекта, работающих с такой информацией.

В рамках установленного на объекте режима секретности проводятся все остальные мероприятия по защите сведений, составляющих государственную тайну.

2.3. Конфиденциальная информация и её защита

Коммерческая тайна. Служебная тайна. Профессиональные тайны. Персональные данные.

Основные термины и понятия:
Коммерческая (служебная) тайна
Персональные данные
Профессиональная тайна

С развитием информационного общества проблемы, связанные с защитой конфиденциальной информации, приобретают всё большее значение. В настоящее время в российском законодательстве данные вопросы полно и системно не решены. Развернутая классификация конфиденциальной информации, как уже говорилось выше, приводится в перечне сведений конфиденциального характера, установленном Указом Президента РФ от 6 марта 1997 г. № 188. Далее мы рассмотрим более подробно некоторые виды конфиденциальной информации.

Коммерческая тайна

Коммерческая деятельность организации тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразной информации. Защите подлежит не вся информация, а только та, которая представляет ценность для организации. При определении ценности коммерческой информации необходимо руководствоваться такими её свойствами, как полезность, своевременность и достоверность.

Полезность информации состоит в том, что она создает субъекту выгодные условия для принятия оперативного решения и получения эффективного результата. В свою очередь полезность информации зависит от своевременного её получения и доведения до исполнителя. Из-за несвоевременного поступления важных по своему содержанию сведений часто упускается возможность заключить выгодную торговую или иную сделку.

Критерии полезности и своевременности тесно взаимосвязаны и взаимозависимы с критерием достоверности информации. Причины возникновения недостоверных сведений различны: неправильное восприятие (в силу заблуждения, недостаточного опыта или профессиональных знаний) фактов или умышленное, предпринятое с определенной целью, их искажение. Поэтому, как правило, сведения, представляющие коммерческий интерес, а также источник их поступления должны подвергаться перепроверке.

Коммерческая (служебная) тайна негосударственной организации – *сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб её интересам.*

Собственник коммерческой информации на основании совокупности перечисленных критериев определяет её ценность для своей хозяйственной деятельности и принимает соответствующее оперативное решение.

В зарубежной экономической литературе коммерческая информация рассматривается не в качестве средства извлечения

прибыли, а, прежде всего, как условие, способствующее или препятствующее получению прибыли. Особо подчеркивается наличие стоимостного фактора коммерческой информации, т.е. возможность выступать в качестве предмета купли-продажи. Поэтому важное значение в условиях развития многообразных форм собственности имеет вопрос об определении принадлежности информации на правах интеллектуальной собственности конкретному субъекту предпринимательства, а в итоге – о наличии у него прав на её защиту.

Определение и вопросы гражданско-правовой защиты служебной и коммерческой тайны в российском законодательстве не различаются и рассмотрены в ст. 139 части первой ГК РФ, называющейся «Служебная и коммерческая тайна»:

«Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране её конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору».

Обеспечение защиты государственной тайны не имеет прямого отношения к защите коммерческой тайны. Однако следует указать на некоторые возможные исключения. Под защиту государства может быть взята коммерческая информация, оцененная как особо важная не только для её собственника, но и для государства, когда не исключено, что к ней может проявить интерес иностранная спецслужба. Вопрос о подобной защите должен решаться на договорной основе между предпринимате-

лем и органом федеральной безопасности с обозначением пределов и функций профессиональной деятельности последних. Что касается собственно коммерческой тайны, то она специальной уголовно-правовой и режимной защитой не обладает.

Действительная или потенциальная коммерческая ценность информации во многом носит субъективный характер и позволяет предпринимателю ограничивать доступ к практически любым сведениям, используемым в предпринимательской деятельности, за исключением сведений, определяемых нормативно-правовым и актами.

Какие сведения не могут составлять коммерческую тайну? В постановлении Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» обозначены:

- учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

- документы, дающие право заниматься предпринимательской (деятельностью (регистрационные удостоверения, лицензии, патенты);

- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

- документы о платежеспособности;

- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

- документы об уплате налогов и обязательных платежах;

- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Этим же нормативным актом запрещено государственным и муниципальным предприятиям до и в процессе их приватизации относить к коммерческой тайне данные:

- о размерах имущества предприятия и его денежных средствах;
- о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;
- о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров;
- о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

Следует отметить, что ограничения, вводимые на использование сведений, составляющих коммерческую тайну, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при формировании трудовой деятельности организации, персонала подразделений, а также при их сотрудничестве с работниками других организаций.

Целью таких ограничений является предотвращение разглашения, утечки или несанкционированного доступа к конфиденциальной информации. Ограничения должны быть целесообразными и обоснованными с точки зрения необходимости обеспечения информационной безопасности. Не допускается использование ограничений для сокрытия ошибок и некомпетентности руководства организации, расточительства, недобросовестной конкуренции и других негативных явлений в деятельности организации, а также для уклонения от выполнения договорных обязательств и уплаты налогов.

Служебная тайна

Если основной целью обеспечения конфиденциальности информации, составляющей коммерческую тайну, является обеспечение конкурентного превосходства, то защита конфиденциальности служебной тайны, хотя и может затрагивать коммерческие интересы организации, но главной задачей имеет обеспечение интересов клиентов либо собственных интересов,

непосредственно не связанных с коммерческой деятельностью. Так, к служебной, а не к коммерческой, тайне следует отнести сведения, касающиеся мер по обеспечению безопасности сотрудников организации, охране складских и иных помещений и др., прямо не связанные с осуществлением предметной деятельности.

В настоящее время институт служебной тайны в отечественном праве является наименее разработанным. В этой проблеме можно выделить три ряда вопросов.

Во-первых, на законодательном уровне требуют урегулирования вопросы «пограничных» и «производных» сведений. «Пограничные» сведения – это такая служебная информация в любой отрасли науки, техники, производства и управления, которая при определенном обобщении и интеграции становится государственной тайной. «Производные» сведения – служебная информация, полученная в результате дробления сведений, составляющих государственную тайну, на отдельные компоненты, каждый из которых не может быть к ней отнесен.

Во-вторых, особого правового регулирования требует защита сведений, образующихся в деятельности органов государственной власти и управления. Для формирования административно-правового института служебной тайны следует принять специальный закон, действие которого должно распространяться на все уровни системы государственного управления.

В-третьих, требует защиты определенная категория значимых сведений субъектов гражданско-правовых отношений. Здесь имеется в виду правовая защита сведений, которые в деятельности организаций не могут быть отнесены к коммерческой тайне, несмотря на то, что в ГК РФ понятие служебной тайны напрямую связано с действительной или потенциальной коммерческой ценностью информации.

Следует заметить, что в настоящее время практикуется упрощенный подход: любые сведения о предпринимательской деятельности организации, доступ к которым ограничен, относят к коммерческой тайне. Однако при таком подходе могут возникнуть трудности определения материального ущерба и упущенной выгоды при неправомерном распространении конфиденциальной информации, например сведений о режиме охраны организации или других аспектах её функционирования,

напрямую не связанных с осуществлением предметной деятельности. Вместе с тем указанные сведения необходимо защищать, т.к. от ограничения доступа к ним в значительной степени зависит коммерческий успех организации.

Профессиональные тайны

В соответствии с действующим законодательством к профессиональной тайне относится информация, связанная со служебной деятельностью медицинских работников, нотариусов, адвокатов, частных детективов, священнослужителей, работников банков, загсов, учреждений страхования. В качестве субъекта профессиональной тайны может выступать как юридическое, так и физическое лицо.

> **Профессиональная тайна** – *информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций.*

Сохранение в тайне сведений, полученных в связи с выполнением профессиональных функций, вызвано в первую очередь нормами профессиональной этики, а не собственными коммерческими интересами предпринимателя или организации. Соответствующий правовой статус рассматриваемым нормам придает их законодательное закрепление.

1) **банковская тайна**. Понятие банковской тайны, в соответствии со ст. 857 ГК РФ, охватывает сведения о банковском счёте, вкладе, операциях по счёту, а также сведения о клиентах банка.

Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

ФЗ «О банках и банковской деятельности» определяет обязанности субъектов, категории информации и основания, по которым сведения предоставляются заинтересованным органам государственной власти, организациям и лицам. Кредитная организация, Банк России гарантируют тайну об операциях, о счётах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счётах и вкладах её клиентов и корреспондентов, а также об

иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Банк России не вправе разглашать сведения о счётах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Таким образом, кредитная организация вправе относить к банковской тайне любые сведения, за исключением прямо указанных в Законе.

2) **нотариальная тайна**. Тайна является специфическим правилом нотариальных действий. В соответствии со ст. 5 Основ законодательства РФ о нотариате нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных Основами. Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.

3) **процессуальные тайны** обычно делят на два вида: следственную тайну и тайну совещания судей.

Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам (ст. 310 УК РФ «Разглашение данных предварительного расследования»). Сведения о ходе предварительного расследования могут быть преданы гласности только с разрешения прокурора, следователя или лица, производящего дознание. Такая информация может касаться как характера производимых следственных действий, так и доказательственной базы, перспектив расследования, круга лиц, участвующих в расследовании. Важно отметить, что законодательно не закреплен перечень сведений, составляющих следственную тайну. Это означает, что прокурор, следователь или лицо, производящее дознание, могут по своему усмотрению устанавливать, какая информация о предварительном расследовании может быть специально охраняемой, а какая – нет.

Тайна совещания судей. Для всех четырех видов существующих в отечественном судопроизводстве процессов преду-

смотрена определенная процедура обеспечения независимости и объективности вынесения решения по делу. Эта процедура имеет одной из целей запрет на разглашение информации о дискуссиях, суждениях, результатах голосования, которые имели место во время совещания судей. Обеспечение тайны совещания судей устанавливается ст. 193 Гражданским Процессуальным Кодексом (ГПК) РФ, ст. 70 Федерального конституционного закона «О Конституционном суде Российской Федерации», ст. 124 Арбитражного процессуального кодекса Российской Федерации.

4) **врачебная тайна**. Согласно ст. 61 Основ законодательства РФ об охране здоровья граждан информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

5) **адвокатская тайна**. В соответствии с ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат, помощник адвоката и стажер адвоката не вправе разглашать сведения, сообщенные доверителем в связи с оказанием ему юридической помощи. Причем доверительные сведения, полученные адвокатом, могут быть как в виде документов, так и в устном виде. Законом установлены гарантии независимости адвоката. В частности, адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в связи с исполнением им обязанностей защитника или представителя (ст. 15 Закона).

6) **тайна страхования.** Институт страховой тайны во многих отношениях схож с институтом банковской тайны. Тайну страхования, в соответствии со ст. 946 ГК РФ, составляют полученные страховщиком в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными ст. 139 или ст. 150 ГК РФ.

Согласно ст. 8 Закона РФ «Об организации страхового дела в Российской Федерации» в качестве лица, обязанного сохра-

нять тайну страхования, могут выступать как юридические, так и физические лица – страховые агенты и страховые брокеры. Кроме того, в соответствии со ст. 33 указанного Закона должностные лица федерального органа исполнительной власти по надзору за страховой деятельностью не вправе использовать в корыстных целях и разглашать в какой-либо форме сведения, составляющие коммерческую тайну страховщика.

7) **тайна связи.** ФЗ «О связи» в части защиты информации регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами – физическими или юридическими лицами – по средствам связи. При такой постановке вопроса тайна связи становится инструментом обеспечения сохранности конфиденциальной информации.

Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, охраняется Конституцией РФ. Обязанность обеспечения соблюдения тайны связи возлагается на оператора связи, под которым понимается физическое или юридическое лицо, имеющее право на предоставление услуг электрической или почтовой связи. Также операторы связи обязаны соблюдать конфиденциальность сведений об абонентах и оказываемых им услугах связи, ставших известными операторам в силу выполнения профессиональных обязанностей.

8) **тайна усыновления**. Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения). Согласно ст. 155 УК РФ тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления как служебную или профессиональную тайну (судьи, работники местных администраций, органов опеки и попечительства и прочие лица, указанные в ч. 1 ст. 139 СК РФ). Второй – все другие лица, если установлены их корыстные или иные низменные побуждения при разглашении тайны усыновления без согласия обоих усыновителей.

9) **тайна исповеди**. Обеспечение тайны исповеди является внутренним делом священника; юридической ответственности за её разглашение он не несет. Согласно ч. 2 ст. 51 Конституции

РФ и ч. 7 ст. 3 ФЗ «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Персональные данные

В соответствии с ФЗ «О персональных данных» от 27 июля 2006 года № 152 определен круг сведений, которые могут быть отнесены к персональным данным.

> **Персональные данные** – *любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.*

В России нормы, регулирующие вопросы защиты персональных данных, были впервые включены в Конституцию РФ 1993 г. Согласно ст. 23 и 24 Конституции РФ каждый гражданин РФ имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Конституционное положение о недопустимости сбора, хранения, использования и распространения информации о частной жизни лица является одной из гарантий закрепленного в ст. 23 Конституции РФ права на неприкосновенность частной жизни. Оно призвано защитить частную жизнь, личную и семейную тайну от какого бы то ни было проникновения в неё со стороны как государственных органов, органов местного самоуправления, так и негосударственных предприятий, учреждений, организаций, а также отдельных граждан. В соответствии с

ФЗ «Об информации, информационных технологиях и о защите информации» запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Особое значение запрет собирать, хранить, использовать и распространять информацию о частной жизни лица приобретает в связи с созданием информационных систем на основе использования средств вычислительной техники и связи, позволяющих накапливать и определенным образом обрабатывать значительные массивы информации. Порядок доступа к персональным данным граждан (физических лиц) устанавливается ФЗ «О персональных данных». В Уголовном кодексе РФ существуют ст. 137 и 140, устанавливающие ответственность за нарушение неприкосновенности частной жизни.

2.4. Защита интеллектуальной собственности

Международное право в сфере защиты информации. Защита авторских и смежных прав в законодательстве РФ. Объекты авторского права. Субъекты авторского права. Права обладателей авторских прав.

Основные термины и понятия:
Авторские права
Интеллектуальной собственность

Международное право в сфере защиты информации

До середины XIX в. авторское право как таковое не существовало. Право собственности могло распространяться лишь на конкретные овеществленные произведения искусства (картины, скульптуры и т.п.). Начиная с середины XIX в. авторское право становится самостоятельной формой собственности – произведения интеллектуального труда стали отвечать всем признакам товара.

Бернская конвенция «Об охране литературных и художественных произведений» (1886 г.). Работа по созданию правового инструмента по охране авторского права была начата в Брюсселе в 1858 г. на состоявшемся там конгрессе авторов произведений литературы и искусства. Затем последовали конгрессы в

Антверпене (1861 и 1877 г.) и Париже (1878 г.), с 1883 г. работа была продолжена в Берне, где в 1886 г. после трех дипломатических конференций было выработано международное соглашение, получившее название Бернской конвенции об охране литературных и художественных произведений. Соглашение было подписано девятью государствами: Бельгией, Великобританией, Испанией, Италией, Либерией, Гаити, Тунисом, Францией и Швейцарией. Конвенция вступила в силу 5 декабря 1887 г.

Основные положения Конвенции подлежали обязательному включению в национальные законодательства стран-участниц в тех случаях, когда национальные законодательства обеспечивали менее благоприятный режим для обладателей авторских прав. В этом проявилось стремление создателей Конвенции к унификации основных положений авторского права.

Парижская конференция (1896 г.). 15 апреля 1896 г. в Париже состоялась первая конференция по изменению Конвенции 1886 г. В конвенцию было включено понятие «публикация», определенное как выпуск копий. Таким образом, представление и исполнение драматических, драматическо-музыкальных и музыкальных произведений, выставки произведений искусства к публикации не относились. Было также принято уточнение к ст. 3, в соответствии с которым охрана предоставлялась произведению, впервые опубликованному в стране-участнице Конвенции даже в том случае, когда автор был гражданином страны, не входящей в Бернский союз. Территориальный принцип Конвенции оставался неизменным, однако акцент был перенесен с издателя на автора произведения.

Берлинская конференция (1908 г.). Результатом работы конференции явился почти полный пересмотр всех основных положений Бернской конвенции. Новая редакция содержала 30 статей, и основные нововведения относились к следующим проблемам.

Конвенция 1886 г. ставила охрану авторского права в зависимость от условий выполнения формальностей, предусмотренных в стране первой публикации. На Берлинской конференции было решено отказаться от всех формальностей даже в том случае, если в стране первой публикации они существуют.

Берлинский вариант Конвенции более полно определил и существенно расширил круг объектов охраны, включив в него

произведения хореографии и пантомимы, кинематографии, фотографии и архитектуры. Были признаны права композиторов на разрешение адаптировать их произведения для исполнения аппаратами механического воспроизведения и их публичное исполнение.

Правила, регламентирующие право перевода, были расширены. Берлинская конференция признала их действительность на протяжении всего срока действия авторского права без всяких ограничений.

Срок охраны авторского права был установлен равным 50 годам, исчисляемым со дня смерти автора. Правило не носило обязательный характер – допускались различия в сроках охраны авторских прав, определяемые законом страны, где ищется защита.

Конвенция более четко определила понятия литературного и художественного произведений и закрепила положение о том, что они должны охраняться во всех странах-участницах с обязательным отражением этого в национальных законодательствах.

Римская конференция (1928 г.). Римская конференция проходила в период бурного развития средств массовой информации и коммуникаций. Это нашло отражение в признании охраны прав авторов при трансляции по радио их произведений, в расширении числа объектов охраны, признании личных прав автора и т.п.

Уровень охраны авторского права был повышен в связи с включением в число объектов авторского права устных литературных произведений (лекций, речей, проповедей и т.п.). К числу наиболее важных нововведений следует отнести признание так называемых личных прав автора, которые сохраняются за ним и при отчуждении имущественных прав (издание, публикация, постановка и т.п.).

Брюссельская конференция (1948 г.). Бернская конвенция подверглась существенным изменениям в Брюсселе в 1948 г. Основной целью конференции было стремление добиться более полной унификации правил Конвенции и национальных законодательств, а также учесть новые условия научного и технического развития. Унификация правил применения Конвенции

была достигнута путем усиления принципа её главенства над национальными законодательствами.

Всемирная конвенция об авторском праве (1952 г.). Говоря о причинах принятия Всемирной конвенции об авторском праве, следует иметь в виду прежде всего стремление к этому Соединенных Штатов Америки и ряда других стран, которые хотели иметь соглашение с как можно меньшим количеством императивных условий и формальностей. Всемирная конвенция об авторском праве была принята на состоявшейся в Женеве в сентябре 1952 г. межправительственной конференции с участием представителей 50 стран. Конвенция вступила в силу в сентябре 1955 г.

Женевская конвенция об авторском праве содержит общую декларацию о стремлении стран-участниц конференции создать международно-правовой инструмент, приемлемый для возможно более широкого крута стран и направленный на облегчение распространения произведений интеллектуального творчества в целях лучшего международного взаимопонимания.

Стокгольмская конференция (1967 г.). К этому времени на международной арене появилось большое количество развивающихся стран с их специфическими нуждами и проблемами, которые стремились понизить уровень охраны авторских прав с целью получения свободного доступа к произведениям науки и культуры. Добившиеся высокого уровня охраны авторских прав, развитые капиталистические страны боялись наметившейся тенденции и всячески ей противились. Для сохранения прежнего уровня охраны авторского права предполагалось пойти на сужение границ Бернского союза. Россия присоединилась к Бернской конвенции лишь спустя почти 100 лет после её первого опубликования, в ноябре 1994 г.

Постановлением Правительства РФ от 3 ноября 1994 г. №1224 Российская Федерация присоединилась к Бернской конвенции об охране литературных и художественных произведений в редакции 1971 г. и Всемирной конвенции об авторском праве в редакции 1971 г.

Защита авторских и смежных прав в законодательстве РФ

В настоящее время положение с охраной и защитой прав на интеллектуальную собственность в России характеризуется как весьма тревожное.

Высокая доходность и доступность интеллектуальной собственности стала особенно привлекательной для дельцов «теневой» экономики. Преступность в данной сфере приняла устойчивые организационные формы. Налажены нелегальные каналы быстрого получения экземпляров новых программных продуктов, их взлома в случаях, когда они защищены ключами аппаратной защиты или программными средствами, а также получения новинок аудио-видеопродукции, организованы подпольные технологические линии по тиражированию носителей программ для ЭВМ и аудио-видеокассет, установлены криминальные связи с легальными заводами-производителями компьютерных носителей (компакт-дисков) и по изготовлению крупных партий контрафактного программного обеспечения, аудио-видеопродукции и производству дополнительных (официально не учтенных) тиражей легальной продукции без ведома правообладателя, созданы и действуют оптовые и розничные сбытовые сети.

В отличие от темпов развития законодательства, защищающего авторские права на объекты интеллектуальной собственности, организованная преступность в этой сфере развивается довольно стремительно. Этому способствуют: извлечение из данной деятельности крупной прибыли при минимальных издержках; коррумпированные связи дельцов в государственных органах, в том числе и правоохранительных; несовершенство законодательства и низкий уровень правосознания общества.

Интеллектуальной собственность – *совокупность исключительных прав на результаты интеллектуальной деятельности, а также на некоторые иные приравненные к ним объекты, такие как средства индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг).*

Понятие «интеллектуальная собственность» включает в себя не только авторские права и права на промышленную собственность, но и права на средства индивидуализации товаров и услуг. Кроме этого, имеются специальные законы о специфич-

ных объектах интеллектуальной собственности – топологии интегральных микросхем и селекционных достижениях.

В юридической литературе существуют и другие мнения о понятии «интеллектуальная собственность». Под интеллектуальной собственностью иногда понимают нематериальные объекты авторского и патентного права, иногда их ещё называют «промышленная собственность» или «литературная собственность». Однако произведение (изобретение, товарный знак, фирменное наименование и т.д.), охраняемое авторским и патентным правом, имеет такие особенности духовного порядка, которые не позволяют отождествить его с вещью. Материальное воплощение идей и образов представляет собой «вещь» настолько условную, что по отношению к праву на объект любого творческого произведения правильнее применять термин «интеллектуальные права».

Авторское и патентное права, специфическим объектом которых как раз и является творческое произведение, регулируют данные отношения настолько своеобразно, что становится невозможным даже проведение аналогий между нормами о праве собственности и нормами об интеллектуальных правах. Однако следует отметить, что правовой режим охраны нематериальных объектов выполняет в отношении нематериальных объектов ту же функцию, что и право собственности в отношении материальных объектов (вещей), устанавливает абсолютное право, дающее возможность субъекту (обладателю права) вводить объект в хозяйственный оборот.

Понятие «право собственности» в объективном смысле представляет собой совокупность правовых норм, регулирующих отношения собственности в данном обществе и действительных для всех членов общества, а нарушение этих норм влечет за собой применение принудительных санкций государства.

Право интеллектуальной собственности не является разновидностью права собственности. Это два различных правовых института. Под интеллектуальной собственностью понимаются исключительные права на результаты интеллектуальной деятельности, т.е. на нематериальные объекты, тогда как право собственности относится к вещным правам.

В целях обеспечения защиты авторских, издательских, иных прав на интеллектуальную собственность принят пакет

специальных законов об охране результатов интеллектуальной деятельности. К основным из них следует отнести следующие законы РФ:

- Патентный закон (охватывающий отношения, связанные с созданием, использованием и охраной изобретений, полезных моделей и промышленных образцов);
- «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров»;
- «О правовой охране программ для электронных вычислительных машин и баз данных»;
- «О правовой охране топологий интегральных микросхем»;
- «Об авторском праве и исключительных правах».

Защита прав на результаты интеллектуальной деятельности осуществляется в судебном (общем) и административном (специальном, применяемом в прямо указанных законом случаях) порядке.

Конституция РФ гарантирует каждому свободу литературного, научного, технического и других видов творчества, при этом подчеркивается, что интеллектуальная собственность охраняется законом. Одной из гарантий реализации авторских и смежных прав, декларированной ст. 44 Конституции РФ, является уголовно-правовая защита этих прав, установленная ст. 146 УК РФ.

Действующий УК РФ предусматривает уголовную ответственность за преступления в сфере интеллектуальной собственности по ст. 146 «Нарушение авторских и смежных прав», ст. 147 «Нарушение изобретательских и патентных прав», ст. 180 «Незаконное использование товарного знака».

Правоприменительная практика российского законодательства, защищающего объекты интеллектуальной собственности, окончательно ещё не сложилась. Но в целом борьба с преступлениями в сфере интеллектуальной собственности в ближайшем будущем приобретет ещё большую актуальность, т.к. с каждым днем возрастает значимость объектов интеллектуальной собственности, что обусловлено требованиями научно-технического прогресса, экономическим и социальным развитием России.

Объекты авторского права

Авторское право и регулируемые им имущественные и личные неимущественные отношения связаны с созданием и использованием произведений литературы, науки и искусства. Авторское право как самостоятельный институт решает конкретные задачи, которые включают:

- всемерную охрану имущественных, личных неимущественных прав и законных интересов авторов;
- обеспечение правовыми средствами наиболее благоприятных условий для создания научных и художественных произведений;
- широкое использование их обществом.

Международное авторское право является частью международного частного права. В первоначальном тексте Бернской конвенции 1886 г. понятие «литературные и художественные произведения» было определено через перечисление различных конкретных видов произведений (книги, брошюры, картины и т.п.). Здесь же говорилось о произведениях в области литературы, науки и искусства, которые могут быть выпущены в свет «любым способом издания или воспроизведения». На сегодняшний день круг произведений намного расширился.

Можно выделить ряд основных **объектов** авторского права.

Литературные произведения составляют значительную часть объектов авторского права. Особенность их в том, что мысли, чувства, идеи и образы выражаются посредством слова в оригинальной композиции и оригинальном изложении.

В структуре литературного произведения выделяются тема, материал, идеология, образная система, сюжет, язык, заглавие. Эти элементы литературного произведения разделяются на юридически безразличные, т.е. тема, материал, сюжет, идейное содержание, и юридически значимые – образная система и язык. Использование значимых элементов произведения в ряде случаев требует согласия автора.

Литературная обработка – особый объект авторского права. Она представляет собой музыкальную или литературную обработку произведений авторов, которые в силу некоторых причин (отсутствие навыков и др.) не в состоянии сами привести свое произведение в законченный вид. Кроме того, обработке могут подвергаться народные произведения, произведения не-

известных авторов и т.д. Записанный и обработанный литературный материал должен отвечать требованиям, предъявляемым законом к литературным и музыкальным произведениям.

Музыкальные произведения выражаются в сочетании звуков, образующих мелодию и связанных ритмом и гармонией. Они имеют форму ораторий, симфоний, песен и т. п. Кроме музыкальных произведений существуют также музыкально-драматические произведения, которые создаются на литературно-драматической основе (либретто) и исполняются на сцене в виде опер, балетов, оперетт.

Музыкальные произведения записываются композитором особыми знаками, позволяющими фиксировать его творческий замысел. Нотная запись музыкального произведения образует клавир, представляющий собой переложение музыкального произведения для фортепиано, или же партитуру, содержащую все партии многоголосного музыкального произведения. Музыкальное произведение может фиксироваться также на аудионосителях (кассеты, компакт-диски и т.п.).

Обработка чужих произведений, оркестровка, переложение относятся к объектам авторского права, если они содержат элемент творчества.

Хореографические произведения, или пантомимы, – произведения искусства, создаваемые при помощи пластических движений человеческого тела. В сочетании с музыкой хореографическое произведение образует музыкально-сценическое произведение. В связи с тем, что хореографические произведения довольно сложно закрепить с помощью каких-то особых знаков на бумаге, для этих целей, как правило, используют фото-, кино- и видеозапись.

Произведения изобразительного искусства – это произведения живописи, графики, скульптуры, декоративно-прикладного искусства и т.п. Художники, скульпторы создают оригинальные произведения, которые могут воспроизводиться путем изготовления копий либо самими авторами, либо иными лицами.

Архитектурные произведения (проекты) также являются объектами авторского права. Они представляют собой синтез инженерного искусства, бионики, живописи, скульптуры, науки, архитектуры. В них слиты наука, техника, искусство. Эскизный

архитектурный проект, в котором воплощается замысел автора, содержит решения будущего произведения, внутреннее развитие его сочлененных пространств, их объёмы, фактуру и цвет. На основе эскизного архитектурного проекта строятся здания, сооружения, комплексы и т. п.

Аудиовизуальные произведения – достаточно широкая категория, охватывающая многообразные произведения для кино, телевидения, радио, интерактивных сетей и т. п.: сценарии, сценарные планы, тексты песен, кинофильмы, телепередачи, радиопередачи, заставки и многое другое. Данная категория произведений, как правило, закрепляется на аудио-, кино- и видеоносителях (пленка, кассеты, цифровые носители и т.п.).

Программные продукты для средств вычислительной техники могут представлять собой как отдельные прикладные программы (текстовые редакторы, компиляторы и т.п.), так и базы данных, энциклопедии, мультимедийные программы. Кроме того, особенность этой категории заключается в том, что в программах для ЭВМ может иметь место использование других объектов авторского права, это могут быть произведения литературы, музыкальные произведения, произведения изобразительного искусства, кинематографии, а также многое другое. В связи со стремительным прогрессом в области использования вычислительной техники закономерно ожидать появления новых норм внутригосударственного и международного права, направленных на разрешение множества коллизий.

Все вышеперечисленные объекты авторского права можно отнести к категории оригинальных произведений, создаваемых авторами. Кроме них конвенционной охране подлежат также зависимые произведения, возникшие на основе существующих оригинальных произведений. Эти произведения появляются в результате перевода (с иностранного языка), переделки, составительства.

Зависимость перевода литературного, художественного, научного произведения от оригинала не лишает его самостоятельности. Конвенция относит переводы к объектам авторского права, сохраняя для них те же критерии охраноспособности, что и для других произведений. Если же переводчик ограничивает свою работу лишь подбором равнозначных слов к языку оригинала, то подобный перевод («подстрочник») не может быть объ-

ектом авторского права. Перевод, выполненный с согласия автора или его правопреемников одним лицом, не может препятствовать другому лицу осуществлять новый перевод этого же произведения.

К объектам авторского права относятся ***сборники произведений***. В сборники могут включаться произведения, не являющиеся предметом чьего-либо авторского труда (законы, статистика, судебные решения и т.д.), а также произведения отдельных авторов. Творческий характер труда составителя заключается в подборе и расположении материала. Авторское право составителя сборника не может мешать другому лицу самостоятельно систематизировать, обрабатывать и выпускать в свет те же произведения.

Научное произведение – это определенная система понятий. Научное произведение может быть выражено в форме учебника, монографии, статьи и т.д. Существуют и другие формы воплощения научных произведений: чертежи, планы, эскизы, модели, компьютерные программы, различного рода карты и т.п.

Основное отличие авторского права от режима правовой охраны других результатов интеллектуальной деятельности состоит в том, что произведение литературы, науки и искусства становится объектом авторского права в силу самого факта его создания автором без какой-либо регистрации, оформления или соблюдения иных формальностей.

Субъекты авторского права

Субъектами авторского права выступают лица, создавшие творческим трудом произведения литературы, науки и искусства (авторы). Возникновение субъективных авторских прав у гражданина не зависит от возраста, имущественного положения, места создания и выпуска произведения в свет и т.п. Субъектом авторских прав может стать даже человек, признанный судом недееспособным (например, по причине душевной болезни).

Иностранный гражданин может быть субъектом российского авторского права, если его произведение впервые выпущено в свет на территории страны либо не выпущено, но находится на её территории в какой-либо объективной форме. Когда произведение иностранного автора впервые выпущено в свет за границей или находится там в объективной форме, этот автор становится субъектом российского авторского права только в

силу заключенных РФ соглашений и в пределах, ими установленных.

Наряду с авторами произведений к субъектам авторского права относятся лица (граждане и организации), которые не участвуют в творческом создании произведений литературы, науки и искусства. Их называют правопреемниками. К правопреемникам переходит определенный круг авторских правомочий по использованию произведений автора, основанием такого перехода служит закон, наследование или договор с автором.

Как правило, автором того или иного произведения выступает одно лицо, которое создало его творческим трудом. Однако в работе над произведением литературы, науки и искусства могут быть объединены усилия нескольких лиц – соавторов.

Особое место в международной системе охраны авторских прав занимают обладатели так называемых смежных прав. Это новое понятие для нашего права, а в некоторых странах понятие «обладатели смежных прав» вообще не используется. К такого рода субъектам относится достаточно широкий круг лиц, таких как режиссеры, актеры, исполнители, продюсеры и т.п.

В международном праве охрана прав, примыкающих к авторским, осуществляется в соответствии с международной конвенцией об охране прав артистов, исполнителей, изготовителей фонограмм и вещательных организаций, подписанной в Риме в 1961 г. Эта Конвенция представляет собой попытку сбалансировать охрану всех категорий субъектов авторского права.

Права обладателей авторских прав

Автором произведения признается гражданин, творческим трудом которого оно создано.

Автору произведения принадлежит исключительное право на свое произведение, включающее:

- право авторства;
- право на имя;
- право на неприкосновенность произведения;
- право на опубликование произведения;
- право на использование произведения (право осуществлять или разрешать его воспроизведение любыми способами – в печати, путем публичного исполнения, передачи в эфир, в видео- и звукозаписи, по кабельному телевидению, с помощью

спутников и иных технических средств; перевод, переработку произведения; распространение экземпляров воспроизведенного произведения; реализацию архитектурного и дизайнерского проекта и т.п.);

- право на вознаграждение за разрешение использовать и использование произведения.

Автор может передать право на использование своего произведения как на территории своего государства, так и за рубежом любым гражданам и юридическим лицам, в том числе и иностранным.

Авторское право на произведение, созданное совместным творческим трудом двух или более граждан, принадлежит соавторам совместно, независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет также самостоятельное значение.

Взаимоотношения соавторов могут определяться договором между ними. Каждый из соавторов сохраняет авторское право на созданную им часть произведения, имеющую самостоятельное значение, и вправе использовать такую часть произведения по своёму усмотрению.

Составители сборников произведений, которые представляют собой по подбору и расположению материалов результат творческого труда, пользуются авторским правом на сборник при условии соблюдения прав авторов каждого из произведений, включенных в сборник.

Авторы произведений, включенных в сборник, сохраняют авторское право каждый на свое произведение и могут использовать свои произведения независимо от сборника в целом.

Организации, выпускающие в свет энциклопедии, энциклопедические словари, газеты, журналы, периодические и продолжаемые сборники научных трудов и другие периодические издания, пользуются правом на использование издания в целом, если иное не установлено в договорах с авторами, произведения которых включены в такое издание.

Авторы кино-, теле- и видеофильма по авторским договорам передают право на использование фильма его изготовителю в пределах, предусмотренных договором.

Авторы произведений, использованных в фильме, сохраняют авторское право каждый на свое произведение, передают

изготовителю право на его использование и могут использовать произведение независимо от фильма в целом.

К наследникам автора переходит право охраны неприкосновенности произведения, право осуществлять или разрешать его опубликование или использование, а также право на получение вознаграждения за разрешение использовать или использование произведения.

К иным правопреемникам автора, в том числе юридическим лицам, может переходить только право на использование произведения.

Обладатели «смежных прав» имеют следующие права: исполнителям-артистам, режиссерам-постановщикам и дирижерам принадлежат право на имя, право на защиту постановки и исполнения произведения, право осуществлять или разрешать использование постановки и исполнения и право на вознаграждение. Запись исполнения, трансляция и иное использование могут производиться только с согласия исполнителя.

Лицу, создавшему звуко- и видеозапись, принадлежит право осуществлять или разрешать её воспроизведение. Использование звуко- и видеозаписи допускается только с разрешения этого лица или его правопреемника (правообладателя).

Право на звуко- и видеозапись включает право её воспроизведения любыми способами, право её публичного распространения, в том числе передачи за границу, а также право на защиту от импорта и распространения экземпляров записи без разрешения правообладателя. Если право собственности на экземпляр звуко- или видеозаписи принадлежит не её создателю, то исключительное право коммерческого проката сохраняется за лицом, создавшим звуко- или видеозапись.

Организациям эфирного вещания принадлежит право разрешать другим организациям ретрансляцию, запись и воспроизведение их передач. Организациям публичного вещания принадлежит также право разрешать публичное воспроизведение телевизионных передач, если оно производится за плату в местах, доступных неопределенному кругу лиц.

Создатели звуко- и видеозаписей, организации эфирного вещания осуществляют свои права в пределах прав, полученных по договору с автором и исполнителем, а организации эфирного вещания так же, без ущерба правам создателей звукозаписи.

Исполнители осуществляют свои права с соблюдением прав авторов исполняемых ими произведений.

Чтобы защитить своё исключительное право на использование программного продукта, правообладатель может обратиться в суд, арбитражный или третейский суд и требовать возмещения причиненных убытков, в размер которых включается сумма доходов, неправомерно полученных нарушителем, или выплаты нарушителем компенсации, определяемой по усмотрению судебных органов. Помимо возмещёния убытков или выплаты компенсации по усмотрению судебного органа в доход бюджета России может быть взыскан штраф в размере 10% суммы, присужденной в пользу истца.

Судебный орган может вынести решение о конфискации контрафактных экземпляров программного продукта, а также материалов и оборудования, используемых для их воспроизведения, и об их уничтожении либо о передаче их в доход бюджета Российской Федерации, либо истцу по его просьбе в счёт возмещёния убытков.

Тем не менее в настоящее время существующую судебную практику защиты прав правообладателя нельзя, к сожалению, считать совершенной; имеющиеся случаи судебной защиты авторских прав пока ещё редки, однако ситуация меняется – ещё несколько лет назад в судах подобные дела к производству практически не принимались.

Вопросы для самоконтроля

1. Перечислите отрасли права, акты которых включают информационно-правовые нормы.
2. К какой информации, в соответствии с законодательством, не может быть ограничен доступ?
3. Какая информация относится к сведениям конфиденциального характера?
4. Какие сведения относят к сведениям особой важности?
5. Какие сведения относят к совершенно секретным сведениям?
6. Какие сведения относят к секретным сведениям?
7. В сведениях какого характера может содержаться государственная тайна?

8. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?

9. Какие меры включаются в систему защиты государственной тайны?

10. Перечислите основные организационные и технические способы защиты государственной тайны.

11. Каково основное назначение режима секретности?

12. Какие группы мер включает в себя режим секретности?

13. Какие сведения не могут составлять коммерческую тайну?

14. Чем вызвано обязательство сохранения в тайне сведений, составляющих профессиональную тайну?

15. Какой нормативный документ определяет порядок доступа к персональным данным граждан?

16. Перечислите основные объекты авторского права.

17. Что включает в себя исключительное право автора на свое произведение?

ГЛАВА 3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

3.1. Информационная безопасность РФ

Доктрина информационной безопасности РФ. Национальные интересы РФ в информационной сфере. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Основные цели и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ.

Основные термины и понятия:
Доктрина информационной безопасности РФ
Информационная безопасность РФ
Национальные интересы РФ в информационной сфере
Объект информационной безопасности РФ
Угрозы информационной безопасности РФ

Современный этап развития общества характеризуется возрастающей ролью информационных взаимодействий инфраструктур и субъектов, осуществляющих сбор, формирование, распространение и использование информации. Информационная сфера, являясь системообразующим фактором в жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенно зависит от обеспечения информационной безопасности.

Доктрина информационной безопасности РФ

Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Информационная безопасность РФ − *это состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.*

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, духовном обновлении России.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, её использовании в интересах осуществления не запрещённой законом деятельности, физического, духовного и интеллектуального развития, а также в защите процессов переработки информации, обеспечивающей личную безопасность.

Доктрина информационной безопасности РФ была утверждена Президентом Российской Федерации В. В. Путиным 9 сентября 2000 г. и структурно состоит из 4 разделов.

В первом разделе «Информационная безопасность Российской Федерации» приведены национальные интересы Российской Федерации в информационной сфере и пути их обеспечения, указаны виды и источники угроз информационной безопасности РФ, рассмотрено состояние информационной безопасности РФ и намечены основные задачи по ее обеспечению.

Во втором разделе «Методы обеспечения информационной безопасности Российской Федерации» рассматриваются общие методы обеспечения информационной безопасности РФ (правовые, организационно-технические и экономические). Рассмотрены вопросы международного сотрудничества РФ в области обеспечения информационной безопасности. Указаны особенности обеспечения информационной безопасности РФ в различных сферах общественной жизни:

- в сфере экономики;

- в сфере внутренней политики;
- в сфере внешней политики;
- в области науки и техники;
- в сфере духовной жизни;
- в общегосударственных информационных и телекоммуникационных системах;
- в сфере обороны;
- в правоохранительной и судебной сферах.

В третьем разделе «Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по её реализации» приведены основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ.

В четвёртом разделе «Организационная основа системы обеспечения информационной безопасности Российской Федерации» рассматриваются основные функции системы обеспечения информационной безопасности РФ и основные элементы её организационной основы.

Национальные интересы РФ в информационной сфере

В информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности с учётом национальных интересов РФ. Согласно Доктрине информационной безопасности РФ, выделяют **четыре** основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая представляет собой информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о самой государственной политике, её официальной позиции по социально значимым событиям

российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая предусматривает развитие современных информационных технологий, отечественной индустрии информации (средств информатизации, телекоммуникации и связи); обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронного и компьютерного производства.

Четвертая составляющая включает в себя защиту информационных ресурсов от несанкционированного доступа; обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Правовое обеспечение информационной безопасности РФ должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации неукоснительно руководствоваться при решении возникающих в информационной сфере конфликтов законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Виды угроз информационной безопасности РФ

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие **виды**:

1) угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

2) угрозы информационному обеспечению государственной политики Российской Федерации;

3) угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

4) угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики;

- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;

- нарушения технологии обработки информации;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

- компрометация ключей и средств криптографической защиты информации;

- утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- нарушение законных ограничений на распространение информации.

Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К **внешним** источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

- обострение международной конкуренции за обладание информационными технологиями и ресурсами;

- деятельность международных террористических организаций;

- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К **внутренним** источникам относятся:

- критическое состояние отечественных отраслей промышленности;

- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

- недостаточная экономическая мощь государства;

- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Основные цели и задачи обеспечения информационной безопасности РФ

Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития, к которым относятся:

- сохранение и укрепление российской государственности и политической стабильности в обществе;

- сохранение и развитие демократических институтов общества, обеспечение прав и свобод граждан, укрепление законности и правопорядка;

- обеспечение достойной роли России в мировом сообществе;

- обеспечение территориальной целостности страны;

- обеспечение прогрессивного социально-экономического развития России;

- сохранение национальных культурных ценностей и традиций.

В соответствии с указанными приоритетами основными **целями** информационной безопасности РФ являются:

- защита национальных интересов России в условиях глобализации информационных процессов, формирования мировых

информационных сетей и стремления США и других развитых стран к информационному доминированию;

- обеспечение органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов;

- реализация прав граждан, организаций и государства на получение, распространение и использование информации.

К основным **задачам** обеспечения информационной безопасности РФ относятся:

- выявление, оценка и прогнозирование источников угроз информационной безопасности;

- разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов её реализации;

- разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления и предприятий по обеспечению информационной безопасности;

- развитие системы обеспечения информационной безопасности, совершенствование её организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий её нарушения;

- обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

Объекты информационной безопасности РФ

К объектам информационной безопасности РФ относятся:

- информационные ресурсы, независимо от форм хранения, содержащие информацию ограниченного доступа, информацию, составляющую государственную тайну, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания;

- система формирования, распространения и использования информационных ресурсов, включающая информационные системы различного класса и назначения, библиотеки, архивы,

базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий персонал;

- информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;

- система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и пр.), базирующаяся на средствах массовой информации и пропаганды;

- права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования государственных и общественных институтов, а также формирования общественного сознания, отвечающего прогрессивному развитию страны.

3.2. Правовое обеспечение информационной безопасности РФ

Правовое обеспечение рассматривается как приоритетное направление формирования механизмов реализации политики обеспечения информационной безопасности в РФ и включает в себя:

1) нормотворческую деятельность по созданию законодательства, регулирующего отношения в обществе, связанные с обеспечением информационной безопасности;

2) исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации и защиты информации органами государственной власти и управления, организациями (юридическими лицами), гражданами.

Нормотворческая деятельность в области обеспечения информационной безопасности предусматривает:

- оценку состояния действующего законодательства и разработку программы его совершенствования;

- создание организационно-правовых механизмов обеспечения информационной безопасности;

- формирование правового статуса всех субъектов в системе информационной безопасности, пользователей информационных и телекоммуникационных систем и определение их ответственности за обеспечение информационной безопасности;

- разработку организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учётом всех видов (категорий) информации;

- разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействия угроз, восстановления нарушенного права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность предусматривает разработку процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и нарушившим регламент информационных взаимодействий, а также правонарушения с использованием незащищенных средств информатизации, разработку составов правонарушений с учётом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений права: соблюдение законности, обеспечение баланса интересов отдельных субъектов и государства, неотвратимость наказания.

Соблюдение законности предполагает наличие законов и иных нормативных установлений, их применение и исполнение субъектами права в области информационной безопасности. Законодательная и нормативно-правовая база в сфере информации и информационной безопасности в РФ включает в себя:

1. Законы Российской Федерации:

- Конституция РФ;
- «О банках и банковской деятельности»;
- «О безопасности»;
- «О внешней разведке»;
- «О государственной тайне»;

- «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

- «О закрытом административно-территориальном образовании»;

- «О милиции»;

- «О правовой охране программ для электронных вычислительных машин и баз данных»;

- «О правовой охране топологий интегральных микросхем»;

- «О связи»;

- «О сертификации продукции и услуг»;

- «О средствах массовой информации»;

- «О стандартизации»;

- «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров»;

- «О федеральных органах правительственной связи и информации»;

- «Об авторском праве и смежных правах»;

- «Об архивном фонде Российской Федерации и архивах»;

- «Об информации, информационных технологиях и о защите информации»;

- «Об обороне»;

- «Об оперативно-розыскной деятельности»;

- «Об органах Федеральной службы безопасности в Российской Федерации»;

- «Об обязательном экземпляре документов»;

- «Об участии в международном информационном обмене»;

- «Об электронной цифровой подписи»;

- «Патентный закон».

2. Нормативные правовые акты Президента Российской Федерации:

- Доктрина информационной безопасности РФ;

- Военная доктрина РФ;

- Концепция национальной безопасности РФ;

- «Вопросы межведомственной комиссии по защите государственной тайны»;

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации»;

- «О создании Государственной технической комиссии при Президенте Российской Федерации»;

- «О Государственной технической комиссии при Президенте Российской Федерации»;

- «О некоторых вопросах межведомственной комиссии по защите государственной тайны»;

- «О перечне сведений, отнесенных к государственной тайне»;

- «Об основах государственной политики в сфере информатизации»;

- «Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне»;

- «Об утверждении перечня сведений конфиденциального характера».

3. Нормативные правовые акты Правительства Российской Федерации:

- «О сертификации средств защиты информации»;

- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;

- «Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР»;

- «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;

- «О подготовке к передаче сведений, составляющих государственную тайну, другим государствам»;

- «О лицензировании отдельных видов деятельности».

4. Руководящие документы Гостехкомиссии России:

- «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;

- «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники»;

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

- «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

- «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

- «Защита информации. Специальные защитные знаки. Классификация и общие требования»;

- «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

5. Уголовный кодекс Российской Федерации.

Реализация механизмов правового обеспечения информационной безопасности должна опираться на информатизацию правовой сферы в целом.

3.3. Государственная политика обеспечения информационной безопасности РФ

Основные положения государственной политики обеспечения информационной безопасности РФ. Основные положения государственной политики обеспечения информационной безопасности субъектов РФ.

Основные термины и понятия:
Государственная политика обеспечения информационной безопасности РФ

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной

сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных **принципах**:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государственная политика является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учётом ограничений, предусмотренных действующим законодательством.

Государственная политика исходит из принципа безусловного правового равенства 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 нормативно-правовую базу информационных отношений в обществе, а также осуществляет контроль за безусловным их исполнением.

Государство исходит из того, что информационные ресурсы являются объектом собственности, способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.

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

Исходя из принципа разделения ответственности между органами федеральной, региональной власти и местного самоуправления, государственная политика предусматривает согласованность организационных и технических решений, принимаемых этими органами для обеспечения информационной безопасности в рамках единого информационного пространства России.

Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности.

Основные положения государственной политики обеспечения информационной безопасности РФ

Государственная политика обеспечения информационной безопасности исходит из следующих основных положений:

- ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

- ответственность за сохранность информации, её засекречивание и рассекречивание персонифицируется;

- доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учётом 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 обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

- государство законными средствами обеспечивает защиту общества отложной, 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 информации 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 государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

- государство формирует федеральную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

- государство прилагает усилия для противодействия информационной экспансии ряда развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе изложенных принципов и положений определяются общие направления формирования и реализации политики информационной безопасности в политической, военной, экономической и других сферах деятельности государства.

Государственная политика в качестве механизма согласования интересов субъектов информационных отношений и нахождения компромиссных решений предусматривает формирование и организацию эффективной работы различных советов, комитетов и комиссий с широким представительством специалистов и всех заинтересованных структур. Механизмы реализации государственной политики должны быть гибкими и своевременно отражать изменения, происходящие в политической и экономической жизни страны.

Основные положения государственной политики обеспечения информационной безопасности субъектов РФ

Информационная собственность субъектов РФ является разновидностью государственной собственности субъектов РФ и включает в себя:

- информационную собственность органов власти и управления субъектов РФ;
- информационную собственность предприятий и учреждений, созданных или приобретенных за счёт средств субъектов РФ;
- культурные ценности народов, населяющих территорию субъектов РФ.

Обязанностью органов власти и управления субъектов РФ является защита права информационной собственности, находящейся на территории субъектов РФ, объектов федеральной информационной собственности, информационной собственности органов местного самоуправления, других юридических и физических лиц.

Субъекты РФ обладают всей полнотой информационных прав, действующих в РФ. Эти права от имени субъектов РФ осуществляют их органы государственной власти и управления.

Субъектам РФ гарантируется:

- равное право доступа на российский рынок информации и средств обеспечения информационной безопасности, находящихся в любой форме собственности;
- право использования для решения региональных государственных задач федеральных информационных банков данных с соблюдением установленных правил обеспечения информационной безопасности;

- право проведения самостоятельной внутренней и внешнеэкономической деятельности в сфере информационной безопасности в рамках, определенных федеральными законами;

- право осуществлять защиту своих информационных прав и права информационной собственности как самостоятельно, так и путем обращения в федеральные и международные правозащитные органы.

Более подробная проработка основных направлений региональной политики обеспечения информационной безопасности должна быть осуществлена субъектами РФ с учётом особенностей их территорий, состояния и перспектив развития хозяйственной сферы.

3.4. Государственная система защиты информации РФ

Задачи системы защиты информации РФ.
Структура государственной системы защиты информации РФ.

Основные термины и понятия:
Государственная система защиты информации РФ

Анализ состояния информационной безопасности в стране диктует необходимость реформирования существующей организации обеспечения информационной безопасности в целях создания целостной системы обеспечения информационной безопасности РФ (далее − система).

Система является составной частью общей **системы национальной безопасности страны** и представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих деятельность по обеспечению информационной безопасности на основе единых правовых норм.

Основными **функциями** системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;

- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;

- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;

- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;

- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;

- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и

органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

Задачи системы защиты информации РФ

Основными задачами системы защиты информации РФ являются:

1) проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности.

2) исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение её утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных

программно-технических воздействий в целях разрушения (уничтожения) или искажения информации в процессе её обработки, передачи и хранения.

3) анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок.

4) оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз.

5) контроль состояния защиты информации в органах государственной власти и на предприятиях.

6) организация фундаментальных, поисковых и прикладных научных исследований в области информационной безопасности.

7) обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации и сертификации средств защиты информации.

8) осуществление международного сотрудничества в сфере информационной безопасности, представление интересов РФ в соответствующих международных организациях.

Система должна обеспечивать гибкое управление процессами информационной безопасности на государственном, региональном, отраслевом, производственном и пользовательском уровнях.

Масштабность, сложность и разнообразие перечисленных функций требуют создания иерархической организационной структуры, обеспечивающей координацию деятельности всех составляющих системы информационной безопасности.

Структура государственной системы защиты информации РФ

Структуру государственной системы защиты информации составляют:

- органы государственной власти и управления РФ и субъектов РФ, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

- государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

- Государственная техническая комиссия при Президенте РФ;

- Федеральная служба безопасности РФ;

- Министерство внутренних дел РФ;

- Министерство обороны РФ;

- Федеральное агентство правительственной связи и информации при Президенте РФ;

- Служба внешней разведки РФ;

- структурные и межотраслевые подразделения по защите информации органов государственной власти;

- головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по защите информации органов государственной власти;

- предприятия, проводящие работы по оборонной тематике и другие работы с использованием сведений, отнесенных к государственной или служебной тайне, их подразделения по защите информации;

- учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

В соответствии с Указом Президента РФ от 5 января 1992 г. № 9 создана Государственная техническая комиссия при Президенте РФ в целях обеспечения национальной безопасности народов и территорий Российской Федерации в части приоритетов и защиты информации в области обороны, политики, экономики, науки, экологии, ресурсов и противодействия иностранным техническим разведкам.

Гостехкомиссия России, являясь органом государственного управления, осуществляет проведение единой технической политики и координацию работ в области защиты информации, возглавляет Государственную систему защиты информации от технических разведок, несет ответственность за обеспечение защиты информации от иностранных технических разведок и от её утечки по техническим каналам на территории РФ, осуществление контроля эффективности принимаемых мер защиты. Гостехкомиссия России подчиняется непосредственно Президенту РФ.

Особое место в системе информационной безопасности занимают государственные и общественные организации, осуществляющие законный контроль за деятельностью государственных и негосударственных средств массовой информации.

Построение системы осуществляется на основе разграничения предметов ведения и полномочий федеральных и региональных органов государственной власти, с учётом согласованности деятельности территориальных органов федеральной исполнительной власти и органов власти субъектов РФ.

3.5. Международное сотрудничество РФ в области обеспечения информационной безопасности

Международное сотрудничество в области обеспечения информационной безопасности − неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая РФ.

Особенность международного сотрудничества РФ в области обеспечения информационной безопасности заключается в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия». Это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Международное сотрудничество в области защиты информации опирается на нормативно-правовую базу:

- Соглашение с Республикой Казахстан от 13.01.1995 г., г. Москва (Постановление Правительства РФ от 15.05.94 г. № 679);

- Соглашение с Украиной от 14.06.1996 г., г. Киев (Постановление Правительства РФ от 7.06.96 г. № 655);

- Соглашение с Республикой Беларусь (Проект);

- Выдача сертификатов и лицензий при международном информационном обмене (Федеральный закон от 4.07.96 г. № 85-ФЗ).

Основными направлениями международного сотрудничества, отвечающими интересам РФ, являются:

- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских сетях и в каналах информационного обеспечения мировой торговли, к конфиденциальной информации в международных политических, экономических и военных союзах, блоках и организациях, к информации в международных правоохранительных организациях, ведущих борьбу с международной организованной преступностью, международным терроризмом, распространением наркотиков и незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми;

- запрещение разработки, распространения и применения «информационного оружия»;

- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при её передаче по национальным телекоммуникационным сетям и каналам связи;

- координация деятельности правоохранительных органов государств - участников международного сотрудничества по предотвращению компьютерных преступлений;

- участие в проведении международных конференций и выставок по проблеме безопасности информации;

- контроль обеспечения безопасности информации в ходе международного военно-технического сотрудничества, при проведении международных выставок (салонов) вооружения и военной техники.

Особое внимание в ходе сотрудничества должно быть уделено проблемам взаимодействия со странами СНГ с учётом перспектив создания единого информационного пространства

на территории бывшего СССР, в пределах которого используются практически единые телекоммуникационные системы и линии связи.

Для реализации указанных направлений сотрудничества необходимо:

- активное участие России во всех международных организациях, действующих в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты процессов переработки информации;
- расширение применения обмена опытом в области обеспечения информационной безопасности, в том числе через международные и отечественные печатные издания;
- расширение участия российских специалистов в международных конференциях, семинарах, выставках.

Для разработки методологических и научно-технических проблем обеспечения международной информационной безопасности целесообразно создание под эгидой ООН международного научно-исследовательского центра.

3.6. Русский язык как объект национальной безопасности РФ

Основные термины и понятия:
Манипулирование социально-политическое

Русский язык является национально-культурной ценностью и представляет собой объект системы национальной безопасности. В Концепции национальной безопасности РФ указывается, что «духовное обновление общества невозможно без сохранения роли русского языка как фактора духовного единения многонациональной России».

Сегодня существует ряд угроз сохранности русского языка, к которым относятся:

1) засорение русского языка терминами и словесными оборотами иностранного происхождения, не свойственными традициям русской словесности;

2) вытеснение русского языка из зоны «дальнего зарубежья» и всё большее ограничение его использования в качестве одного из мировых языков международного общения;

3) широкое использование в русской речи слов и оборотов жаргонного характера;

4) активное сокращение русскоязычного информационного пространства в «ближнем зарубежье», т.е. в государствах СНГ.

Сохранять родной язык необходимо в виду следующих обстоятельств:

- В любом языке содержится больше исторической и культурной информации о его носителе, чем в самом народе, если «вживую» изучать его нравы, традиции, обычаи.

- Поняв язык, можно осознать нормы культуры, конкретные особенности взаимоотношений человека и социальной общности, в которую он включен, проследить изменения в отношении к чему-либо.

- Вместе с гибелью языка рушится жизненный мир: традиции, обычаи, культурная самобытность народа.

Мышление взрослого, нормального человека неразрывно связано с речью. В речи мысль не только формулируется, но и формируется, развивается. Мы мыслим словами, которые произносим вслух или проговариваем про себя, т. е. мышление происходит в речевой форме. Психологи утверждают, что развитие у человека способностей к абстрактному логическому мышлению существенным образом зависит от богатства того языка, на котором он мыслит.

В сознании каждого человека существует нормативная система, которая представляет собой модель мира, задающая программу деятельности и состоящую из неявных и явных норм. Неявные нормы запрограммированы в языке, который отражает сложную структуру бытия, систему отношений и связи между людьми. Слова действуют на сознание человека через ассоциации, порождая поток образов и чувств. Другими словами, «образ мира», который формируется в нашем сознании, определяется не только уровнем наших знаний и идеологическими установками, но также и теми языковыми средствами, с помощью которых он формируется в процессе мышления.

Слова в естественном языке отражают становление национального характера, тип человеческих отношений и отношения человека к миру. Специфика языка определяет специфику осмысления мира. При усвоении родного языка у каждого ребёнка формируется «фильтрующая сетка», заставляющая воспринимать

мир в определенных категориях. Именно в этом смысле надо понимать слова Уорфа: «…мир предстает перед нами как калейдоскопический поток впечатлений, который должен быть организован нашим сознанием, а это значит, в основном – языковой системой, хранящейся в нашем сознании. Мы расчленяем мир, организуем его в понятия и распределяем значения так, а не иначе, в основном, потому, что мы – участники соглашения, предписывающего подобную систематизацию. Это соглашение имеет силу для определенного речевого коллектива и закреплено в системе моделей нашего языка».

Искажения языка происходили всегда и во всех странах, но в наше время это явление приняло угрожающие размеры (процесс стал неуправляемым или, наоборот, очень хорошо спланированным). История показывает, что введение жесткой «языковой цензуры» не приносит ощутимого эффекта, но из этого не следует, что нам нужно пассивно смотреть на происходящее, надеясь, что «язык переживал ещё и не такое, он справится». Во времена Петра I, когда заимствования насаждались в приказном порядке, этот процесс происходил осознанно. В настоящее время ситуация принципиально иная: люди добровольно употребляют заимствованные слова, порой не считаясь ни с какими смыслами (как в случае с употреблением нецензурных слов, которое, как показывают последние научные исследования, негативно отражается даже на физическом здоровье человека).

Методичную и тщательную замену слов русского языка чуждыми нам словами следует рассматривать как манипуляцию сознанием, а не просто «засорение» языка или признак бескультурья. Постепенно происходит искажение модели мира, заложенной структурой родного языка, и навязывание чуждой модели мира, которая призвана обеспечить желаемые (кому-то) типы поведения. Эти действия в специальной литературе называются информационно-психологическими операциями. Ещё в XIX веке Президент Российской Академии наук, государственный секретарь, министр просвещения А. С. Шишков писал, что «не одно оружие и сила одного народа опасна бывает другому; тайное покушение прельстить умы, очаровать сердца, поколебать любовь к земле своей и гордость к имени своему, есть средство надежнее мечей и пушек. Средство медленное, но верное, и, рано или поздно, но цели своей достигает. Мало-помалу налагает

оно нравственные узы, дабы потом наложить и настоящие цепи, зная, что пленник в оковах может разорвать их, может ещё быть горд и страшен победителю, но пленник умом и сердцем остается всегда пленником».

В современном обществе естественный язык стал заменяться искусственным, специально создаваемым. Слова становятся рациональными, они «очищаются» от множества уходящих в глубь веков смыслов. С. Г. Кара-Мурза полагает, что, когда вместо силы главным средством власти стала **манипуляция** общественным сознанием, власть имущим понадобилась полная свобода слова − превращение слова в безличный, неодухотворённый инструмент. «Освобождение» слова означало, прежде всего, устранение из него святости, искры божьей − десакрализацию. Означало и отделение слова от мира (от вещи). Слово, имя, переставало тайно выражать заключенную в вещи первопричину. Отрыв слова (имени) от вещи и скрытого в вещи смысла был важным шагом в разрушении всего упорядоченного Космоса, в котором жил и прочно стоял на ногах человек Средневековья и древности. Начав говорить «словами без корня», человек стал жить в разделенном мире, и в мире слов ему стало не на что опереться.

Манипулирование социально-политическое − *целенаправленное воздействие на общественное мнение и социально-политическое поведение людей с помощью средств массовой коммуникации с целью изменения их сознания, позиции и действий вопреки их интересам.*

По мнению С. Г. Кара-Мурзы, создание «бескорневых» слов (слов-«амёб») стало важнейшим способом разрушения национальных языков и средством атомизации общества. Слова-«амёбы», прозрачные, не связанные с контекстом реальной жизни, перешли в огромном количестве из науки в идеологию, а затем и в наш обыденный язык. «Они настолько не связаны с конкретной реальностью, что могут быть вставлены практически в любой контекст, сфера их применимости исключительно широка (например, слово «прогресс»). Это слова, как бы не имеющие корней, не связанные с вещами (миром). Они делятся и размножаются, не привлекая к себе внимания − и пожирают

старые слова. Они кажутся никак не связанными между собой, но это обманчивое впечатление. Они связаны, как поплавки рыболовной сети − связи и сети не видно, но она ловит, запутывает наше представление о мире».

Важный признак слов-«амёб» − их кажущаяся «научность». Сказав «коммуникация» вместо слова «общение», «мемуары» вместо «воспоминания» или «электорат» вместо «избиратели» начинаешь думать, что мысли якобы подкрепляются авторитетом науки. Здесь уместно привести мнение языковеда и собирателя сказок А. Н. Афанасьева, который подчеркивал значение корня в слове: «забвение корня в сознании народном отнимает у образовавшихся от него слов их естественную основу, лишает их почвы, а без этого память уже бессильна удержать все обилие словозначений; вместе с тем связь отдельных представлений, державшаяся на родстве корней, становится недоступной».

Процесс криминализации нашего общества оказывает влияние и на его язык. Широко употребляемые такие слова как «наезд», «зачистка», «разборка» и т. п. – это прямые заимствования из словаря представителей преступного мира. Криминальное «заражение» речи происходит в основном через СМИ, литературу, кино и музыку. «Жертвами» криминального жанра (боевики, триллеры, фильмы ужасов и т.д.) чаще оказывается молодежь с традиционно высокой степенью внушаемости, психически больные, лица с неустойчивой психикой и отсутствующей сформированной профессиональной мотивацией. Они начинают употреблять слова из криминального словаря, не понимая заложенного в них смысла. Современное «криминальное чтиво» для некоторых категорий людей представляет собой учебники, руководство к действию.

Вопросы для самоконтроля

1. В чём заключаются интересы государства в информационной сфере?
2. В чём заключаются интересы общества в информационной сфере?
3. В чём заключаются интересы личности в информационной сфере?

4. В чём заключаются национальные интересы РФ в информационной сфере?

5. Какие существуют виды угроз информационной безопасности РФ?

6. Перечислите внешние источники угроз информационной безопасности РФ.

7. Перечислите внутренние источники угроз информационной безопасности РФ.

8. Покажите на примерах значение информационной безопасности в обеспечении национальной безопасности государства.

9. Какие нормативные акты обеспечивают информационную безопасность на территории РФ?

10. Какие международные нормативные акты в сфере защиты информации вы знаете?

11. В чём заключается суть государственной политики обеспечения информационной безопасности?

12. Назовите основные функции системы обеспечения информационной безопасности.

13. Из каких элементов состоит Государственная система защиты информации?

14. Почему русский язык рассматривается как объект национальной информационной безопасности?

15. Какие существуют угрозы русскому языку?

16. Как связана речь человека с его мышлением?

СПИСОК ЛИТЕРАТУРЫ

1. *Айков, Д.* Компьютерные преступления / Д. Айков, К. Сейгер, У. Фонсторх. — М. : Мир, 1999. – 351 с.

2. *Аронсон, Э.* Эпоха пропаганды : Механизмы убеждения повседневное использование и злоупотребление / Э. Аронсон, Э. Р. Пратканис. — СПб. : Прайм-ЕВРОЗНАК, 2003. – 384 с.

3. *Бетелин, В.* Информационная безопасность в России: опыт составления карты / В. Бетелин, В. Галатенко // Jet Info № 1. — 1998. — С. 5.

4. Библиотека «ПСИ-ФАКТОРА» [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://psyfactor.org/lybr.htm, свободный. – Загл. с экрана.

5. *Богданов, Е. Н.* Психологические основы «Паблик рилейшнз» : учеб. пособие для студентов вузов / Е. Н. Богданов, В. Г. Зазыкин. – 2-е изд. — СПб. : Питер, 2004. – 204 с.

6. *Бодров, В. А.* Информационный стресс : учеб. пособие для студентов вузов / В. А. Бодров. — М. : ПЕР СЭ, 2000. – 352 с.

7. *Бурлаков, И. В.* Homo Gamer : Психология компьютерных игр / И. В. Бурлаков. – М. : Независимая фирма «Класс», 2000. – 141 с. – (Библиотека психологии и психотерапии, вып. 86).

8. *Гарфинкель, С.* Всё под контролем : Кто и как следит за тобой / С. Гарфинкель ; *пер. с англ.* В. Масянкина. — Екатеринбург : У-Фактория, 2004. – 432 с.

9. *Гафнер, В. В.* Информационная пассивность педагога / В. В. Гафнер // Народное образование. – 2005. – № 2. – С. 235–239.

10. *Гафнер, В. В.* О профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2005. – № 11. – С. 31-34.

11. *Гафнер, В. В.* О профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2005. – № 12. – С. 40-44.

12. *Гафнер, В. В.* Предвидеть и предупреждать. Профессиональная компетентность учителя ОБЖ как психолого- педагогическая проблема / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 9. – С. 15–17.

13. *Гафнер, В. В.* Профессиональная деформация и компетентность педагога / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 10. – С. 22–24.

14. *Гафнер, В. В.* Профессиональная переориентация бывших военнослужащих и проблема становления профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 11. – С. 47–49.

15. *Гафнер, В. В.* Совмещение преподавания: «за» и «против». Совмещение преподавания нескольких учебных предметов как препятствие становления профессиональной компетентности педагога / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 12. – С. 53–55.

16. *Грачев Г. В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – М. : Изд-во РАГС, 1998. – 125 с.

17. *Грачев, Г. В.* Личность и общество: информационно-психологическая безопасность и психологическая защита / Г. В. Грачев. — М. : ПЕР СЭ, 2003. – 304 с.

18. *Грачев Г. В.* Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / Г. В. Грачев, И. К. Мельник. – М. : Алгоритм, 2002. – 288 с.

19. *Гриняев, С. Н.* Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. — Мн. : Харвест, 2004. – 448 с.

20. *Дмитриев, А. В.* Слухи как объект социологического исследования / А. В. Дмитриев // Социс. – 1995. – № 1. – С. 5– 11.

21. *Днепров, А. Г.* Защита детей от компьютерных опасностей (+ CD) / А. Г.Днепров. – СПб. : Питер, 2008. – 192 с.

22. Доктрина информационной безопасности Российской Федерации // Указ Президента РФ № Пр–1895 от 9.09.2000.

23. *Доценко, Е. Л.* Психология манипуляции: феномены, механизмы, защита / Е. Л. Доценко. — М. : Речь, 2004. – 304 с.

24. *Дубин, Б. В.* Слухи как социально-психологический феномен / Б. В. Дубин, А. В. Толстых // Вопросы психологии. – 1993. - № 3. – С. 15-31

25. *Загородников, С. Н.* Основы информационного права : учеб. пособие для студентов вузов / С. Н. Загородников, А. А. Шмелев. — М. : Акад. Проект : Парадигма, 2005. – 192 с.

26. Информационная безопасность России / Ю. С. Уфимцев, Е. А. Ерофеев и др. — М. : «Экзамен», 2003. – 560 с.

27. Информационное оружие, как средство ведения информационного противоборства [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.vrazvedka.ru/main/analytical/lekt-03.shtml, свободный. – Загл. с экрана.

28. Информационно-психологическая и психотронная война : хрестоматия. — Мн. : Харвест, 2003. – 432 с.

29. *Кара-Мурза, С.* Манипуляция сознанием / С. Кара-Мурза. — М. : Эксмо, 2005. – 832 с.

30. *Караяни, А. И.* Слухи как средство информационно - психологического противодействия / А. И. Караяни // Психологический журнал. – 2003. – № 6. – Том 24.

31. *Карпов, А. В.* Психология групповых решений / А. В. Карпов. - М. ; Ярославль, 2000. – 532 с.

32. *Карчевский, Н. В.* Компьютерные преступления: определение, объект и предмет [Электронный ресурс] / Н. В. Карчевский. – Электрон. текст. дан. – Режим доступа: http://www.ifap.ru/pi/05/karchev.htm, свободный. – Загл. с экрана.

33. *Козлов, В. Е.* Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. — М. : Горячая линия-Телеком, 2002. – 336 с.

34. *Колесникова, Т. И.* Психологический мир личности и его безопасность / Т. И. Колесникова. — М. : ВЛАДОС-ПРЕСС, 2001. – 176 с.

35. *Колин, К. К.* Социальная информатика : учеб. пособие для студентов вузов / К. К. Колин. — М. : Акад. Проект : Фонд «Мир», 2003. – 432 с.

36. Концепция национальной безопасности Российской Федерации // Указ Президента РФ № 1300 от 17.12.1997.

37. *Корделлан, К.* Дети процессора: Как Интернет и видеоигры формируют завтрашних взрослых / К. Корделлан, Г. Грезийон ; *пер. с фр.* А. Лущанова. — Екатеринбург : У-Фактория, 2006. – 272 с.

38. *Корнилова, Т. В.* Психология риска и принятия решений / Т. В. Корнилова. – М. : Аспект Пресс, 2003. – 286 с.

39. *Кравченко, А. В.* Интернет и компьютерный терроризм [Электронный ресурс] / А. В. Кравченко. – Электрон. текст. дан.

– Режим доступа: http://www.crime-research.ru/library/kravch.htm, свободный. – Загл. с экрана.

40. *Крысько, В. Г.* Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько. — Мн. : Харвест, 1999. – 448 с.

41. *Куприянов, А. И.* Основы защиты информации : учеб. пособие для студ. высш. учеб. заведений / А. И. Куприянов, А. В.Сахаров, В. А. Шевцов. – М. : Издательский центр «Академия», 2006. – 256 с.

42. *Лисичкин, В. А.* Третья мировая (информационно-психологическая) война / В. А. Лисичкин, Л. А. Шелепин. — М. : Институт социально-политических исследований АСН, 2000. – 304 с.

43. *Макаренкова, В.* Видеоигры в информационной и психологической борьбе / В. Макаренкова // «Зарубежное военное обозрение». – 2005. – № 2.

44. *Мельников, В. П.* Информационная безопасность : учеб. пособие для студентов сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; *под ред.* С. А. Клейменова. — М. : Академия, 2005. – 336 с.

45. *Мельникова, А. А.* Язык и национальный характер. Взаимосвязь структуры языка и ментальности / А. А. Мельникова. – СПб. : Речь, 2003. – 320 с.

46. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов и др. — М. : Издательство «Экзамен», 2004. – 544 с.

47. *Миронова, Т. Л.* Русский язык и национальная безопасность [Электронный ресурс] / Т. Л. Миронова. – Электрон. текстовые дан. – Режим доступа: http://www.lindex.lenin.ru/Lindex4/Text/8770.htm, свободный. – Загл. с экрана.

48. *Моляков, А.* Особенности проявления паники в условиях экологического бедствия / А. Моляков // Психологический журнал. – 1992. – № 2. – Том 13.

49. *Назаретян, А. П.* Агрессивная толпа, массовая паника, слухи / А. П. Назаретян. - СПб. : Питер, 2004. – 192 с.

50. *Нарицын, Н. Н.* Азбука психологической безопасности / Н. Н. Нарицын. — М. : Издательство «Русский журнал», 2000. – 224 с.

51. *Нечаев В. В.* Человек и информационная цивилизация – ритмо–информациологический подход / В. В. Нечаев, А. В. Дарьин // Проблемы информатизации: теоретич. и науч. – практич. журнал / РАН; Мин–во науки и технологий РФ. – 1999. – Вып. 1.

52. *Номоконов, В. А.* Глобализация информационных процессов и преступность [Электронный ресурс] / В. А. Номоконов. – Электрон. текст. дан. – Режим доступа: http://www.crime-research.ru/library/nomokon.htm, свободный. – Загл. с экрана.

53. Об авторском праве и смежных правах // Закон Российской Федерации № 5351-1 от 9.07.1993.

54. Об информации, информационных технологиях и о защите информации // Закон Российской Федерации № 149-ФЗ от 27.07.2006.

55. О государственной тайне // Закон Российской Федерации № 5485–1 от 21.07.1993.

56. *Одинцов, А. А.* Экономическая и информационная безопасность : справ. : учеб. пособие для студентов вузов / А. А. Одинцов. — М. : Экзамен, 2005. – 576 с.

57. Одинцов, А. А. Экономическая и информационная безопасность предпринимательства : учеб. пособие для студентов вузов / А. А. Одинцов. — М. : Академия, 2006. – 336 с.

58. *Оганджанян, Ш.* Чем промывают мозги / Ш. Оганджанян // Всё ясно. – 2006. – № 4 (62). – С. 39-41.

59. Основы информационной культуры : учеб.–метод. пособие / *авт.-сост.* В. И. Золотарева [и др.]. – М. : МИФИ, 2005. – 128 с.

60. *Олпорт, Г.* Становление личности: избранные труды / Г. Олпорт. – М. : Смысл, 2002.

61. Патентный закон // Закон Российской Федерации № 3517-1 от 23.09.1992.

62. *Плаус, С.* Психология оценки и принятия решений / С. Плаус. — М. : Информационно-издательский дом «Филинъ», 1998. – 368 с.

63. *Пономарев, Д. А.* Информационные технологии как криминогенный фактор организованной преступности в условиях глобализации [Электронный ресурс] / Д. А. Пономарев. – Электрон. текст. дан. – Режим доступа: http://www.ifap.ru/pi/06/r16.htm, свободный. – Загл. с экрана.

64. *Почепцов, Г. Г.* Информационные войны / Г. Г. Почепцов. — М. : «Рефл-бук» ; К. : «Ваклер», 2001. – 576 с.

65. *Почепцов, Г. Г.* Психологические войны / Г. Г. Почепцов. — М. : «Рефл-бук» ; К. : «Ваклер», 2001. – 528 с.

66. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов / С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др. ; *под ред.* С. Я. Казанцева. — М. : Академия, 2005. – 240 с.

67. Психология экстремальных ситуаций / *сост.* А. Е. Тарас, К. В. Сельченок. – М. : АСТ, Мн. : Харвест, 2001. – 480 с.

68. *Райнер, П.* Застывший взгляд / П. Райнер. – М.: evidentis, 2003. – 224 с.

69. Растим здоровых, умных, добрых: воспитание младшего школьника : пособ. для средн. и высш. педагогич. учебн. заведений / *сост.* Л. В. Ковинько. — М. : Академия, 1996. – 288 с.

70. Реклама: внушение и манипуляция : учеб. пособие / сост. Д. Я. Райгородский. — Самара : БАРАХ-М, 2001. –752 с.

71. *Розен, Э.* Анатомия слухов: маркетинговые приемы / Э. Розен. – СПб. : Питер, 2006. – 240 с.

72. *Садердинов, А. А.* Информационная безопасность предприятия : учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. – 2-е изд. — М. : Дашков и К, 2005. – 336 с.

73. *Светлакова, Н. Б.* Реклама, которая вас убивает / Н. Б. Светлакова. – М. : Вече, 2007. – 176 с.

74. *Синельников, В. В.* Таинственная сила слова. Формула любви. Как слова воздействуют на нашу жизнь / В. В. Синельников. – М. : ЗАО Центрполиграф, 2006. – 255 с.

75. *Спенсер, Д.* «Да» или «Нет» / Д. Спенсер. — СПб. : Питер Пресс, 1996. – 128с.

76. *Столяренко А. М.* Экстремальная психопедагогика / А. М. Столяренко. – М. : ЮНИТИ-ДАНА, 2002. – 608 с.

77. *Тоффлер Э.* Третья волна. — М.:АСТ, 2004. — 783с.

78. *Тоффлер, Э.* Шок будущего. — М.:АСТ, 2004. — 557 с.

79. *Харрис, Р.* Психология массовых коммуникаций / Р. Харрис. — СПб. : Прайм-ЕВРОЗНАК, 2002. – 448 с.

80. *Черноушек, М.* Психология жизненной среды / М. Черноушек ; *пер. с пол.* И. И. Попа. – М. : Мысль, 1989. - 176 с.

81. *Шелли, Л.* Организованная преступность, терроризм и киберпреступность [Электронный ресурс] / Л. Шелли ; *пер. с*

англ. Т. Л. Тропиной. – Электрон. текст. дан. – Режим доступа: http://crime.vl.ru/docs/stats/stat_123.htm, свободный. – Загл. с экрана.

82. *Шнайер, Б.* Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб. : Питер, 2003. – 368 с.

83. *Щербаков, А. Ю.* Введение в теорию и практику информационной безопасности / А. Ю. Щербаков. — М. : издатель Молгачева С. В., 2001. Нечаев В. В., Дарьин А. В. 352 с.

84. *Эмото, М.* Послания воды: Тайные коды кристаллов льда / М. Эмото; *пер. с англ.* О. Горбунова. — М. : ООО Изд-во «София», 2006. – 96 с.

85. *Эриксен, Т. Х.* Тирания момента. Время в эпоху информации / Т. Х. Эриксен ; *пер. с норв.* – М. : Издательство «Весь Мир», 2003. – 208 с.

86. *Ярочкин, В. И.* Система безопасности фирмы / В. И. Ярочкин. — М. : Ось-89, 2003. -352 с.

87. *Ярочкин, В. И.* Информационная безопасность : учеб. для студентов вузов / В. И. Ярочкин. — М. : Акад. Проект, 2008. — 544 с.

88. Язык наш поводырь наш в рай или ад : сб. статей / *под ред.* Г. Емельяненко. — СПб.: Изд-во Л.С. Яковлевой, 2001. – 336 с.

89. Jet Info, информационный бюллетень [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.jetinfo.ru, свободный. – Загл. с экрана.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Утверждаю
Заместитель Министра образования и науки
Российской Федерации
А. Г. Свинаренко

«31» января 2005 г.
Номер государственной регистрации
715 пед/сп (новый)

Государственный образовательный стандарт Высшего профессионального образования

Специальность 050104.65 «Безопасность жизнедеятельности» Квалификация учитель безопасности жизнедеятельности

Вводится в действие с момента переутверждения
вместо ранее утвержденного (14.04.2000 г., № 379пед/сп)
(выписка)

Москва 2005

ТРЕБОВАНИЯ К ОБЯЗАТЕЛЬНОМУ МИНИМУМУ СОДЕРЖАНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПОДГОТОВКИ ВЫПУСКНИКА ПО СПЕЦИАЛЬНОСТИ 050104.65 «БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ»

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ДПП	**Дисциплины предметной подготовки**	**4334**
ДПП.Ф.00	**Федеральный компонент**	**3934**
ДПП.Ф.16	**Информационная безопасность** Понятие информационной безопасности. Место информационной безопасности в системе национальной безопасности РФ. Основы государственной политики обеспечения информационной безопасности. Международная деятельность по обеспечению информационной безопасности. Законодательство в области информационной безопасности. Основные факторы и ключевые проблемы информационной безопасности. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну. Защита интеллектуальной собственности. Методы и средства защиты электронной информации. Информационные технологии и здоровье. Негативные последствия глобальной информатизации общества, расширение средств массовой информации и рекламы, их дестабилизирующее воздействие на человека.	**140**

СЛОВАРЬ ОСНОВНЫХ ТЕРМИНОВ

Аутентификация – совокупность процедур, цель которых – доказательство того, что идентифицированная сущность является именно той, за которую она себя выдает.

База данных – объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Данные – фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.

Дезинформация – распространение искаженных или заведомо ложных сведений для достижения определенных целей.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и

непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

З**ащита сведений, составляющих государственную тайну, и их носителей** – деятельность органов защиты этой тайны, направленная на обеспечение безопасности информации, отнесенной к государственной тайне, предотвращение её утечки и её максимально эффективное использование.

Знание – форма существования и систематизации результатов познавательной деятельности человека.

Идентификация – отождествление, установление соответствия одной сущности другой.

Интеллектуальной собственность – совокупность исключительных прав на результаты интеллектуальной деятельности, а также на некоторые иные приравненные к ним объекты, такие как средства индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг).

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.

Информационная безопасность – это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность РФ – состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная война – комплекс мероприятий по достижению информационного превосходства путем воздействия на информацию, информационные процессы, информационные системы и компьютерные сети противника при одновременной защите своей информации, информационных процессов, информационных систем и компьютерных сетей.

Информационная картина мира – информационное поле, позволяющее адекватно воспринимать окружающий мир и взаимодействовать с ним, способствовать его и собственному развитию, осуществлять информационный обмен.

Информационная революция – преобразование общественных отношений из-за кардинальных изменений в сфере обработки 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.

Информационная сфера (среда) – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационное общество – концепция постиндустриального общества; ступень развития цивилизации, в которой главными продуктами производства являются информация и знания.

Информационное оружие – комплекс специализированных методов и средств, предназначенных для контроля информационных ресурсов объекта воздействия и временного или безвозвратного вывода из строя функций или служб информационной инфраструктуры в целом или отдельных ее элементов.

Информационный (общественный) резонанс – одновременное повышенное искусственное привлечение средствами массовой информации общественного внимания к тому или иному социальному или политическому событию, сопряжённое с замалчиванием других событий, имеющих равную информативную значимость.

Информационно-психологическая война – открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере, направленные на обеспечение информационного

превосходства над противником и нанесения ему материального, идеологического или иного ущерба.

Информационные продукты (продукция) – документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Информационные процессы – процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

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

Информационные услуги – действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами.

Информация – сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.

Коммерческая (служебная) тайна негосударственной организации – сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб её интересам.

Компьютерное преступление – преступление, совершенное с помощью вычислительной техники и вычислительных сетей, направленное на незаконное похищение информации или приводящее к ее модификации либо разрушению.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Массовая информация – предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Международный информационный обмен – передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу Российской Федерации.

Общественное мнение – состояние массового сознания, заключающее в себе скрытое или явное отношение различных социальных общностей к проблемам, событиям действительности.

Общественное сознание – совокупность идей, взглядов, представлений, существующих в обществе в данный период, в которых отражается социальная действительность.

Пароль – секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

Персональные данные (информация о гражданах) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Принятие решения – процесс выбора варианта действий в имеющейся ситуации из многих возможных.

Пропаганда – воздействие на сознание (подсознание), политические и ценностные ориентации объектов (групп объектов) посредством распространения воззрений, идей, учений с целью формирования мировоззрения, соответствующих интересам воздействующей стороны.

Профессиональная тайна – информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций.

Психологическая война – совокупность различных форм, методов и средств воздействия на людей с целью изменения в желаемом направлении их психологических характеристик (взглядов, мнений, ценностных ориентаций, настроений, мотивов, установок, стереотипов поведения), а также групповых норм, массовых настроений и общественного сознания в целом.

Психологическая операция – проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные враждебные, дружественные иди нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных национальных целей.

Реклама – информация о товарах, различных видах услуги т.п. с целью оповещения потребителей и создания спроса на эти товары, услуги и т.п.

Сервер – аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы предприятия.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Слух – информация, которая распространяется без предоставления общепринятых свидетельств достоверности.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средство массовой информации – периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации.

Учетная запись – информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

Учебное издание

Гафнер Василий Викторович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие
Часть 1

Редактор М. А. Ли-Буланкова

Подписано в печать 01.07.09. Формат 60x90/16.
Бумага для множ. ап. Гарнитура Times New Roman.
Печать на ризографе. Усл. печ. л. 9,8 Уч.-изд. л.
Тираж 500 экз. Заказ 2857

Оригинал-макет отпечатан в отделе множительной техники
Уральского государственного педагогического университета
620017, г. Екатеринбург, просп. Космонавтов, 26.
E-mail: uspu@uspu.ru
E-mail: uralfbg@mail.ru
www.bezopasnost.edu66.ru