**Специальность:\_13.02.07 Электроснабжение (по отраслям)**

**Курс:\_3\_, группа(ы) Э179\_**

**Дисциплина (МДК) Информационные технологии в профессиональной деятельности**

**ФИО преподавателя Талипова А.А.**

# Лекция. Понятие защиты и информационной безопасности

***1. Понятие защиты информации и информационной безопасности***

 Прежде, чем определить само понятие защиты информации и информационной безо­пасности, рассмотрим более общее понятие безопасности.

Общее понятие ***«безопасность»***, широко употребляемое в рус­ском языке, характеризует собой «положение, при котором не угрожает опасность кому-нибудь и чему-нибудь». В. Даль ука­зывал, что безопасность есть отсутствие опасности, сохранность, надежность. По С. Ожегову безопасность — это «состояние, при котором не угрожает опасность, есть защита от опасности».

Однако «защита», «защищенность» — это только одна сторо­на значения слова безопасность. С другой стороны, безопасность означает отсутствие угрозы со стороны объекта, явления или процесса, о безопасности которого идет речь, его безвредность.

В связи с этим, когда мы говорим о безопасности чего-либо или кого-либо, необходимо рассматривать ***два плана***: внутрен­ний — состояние защищенности от внешних угроз и внешний — безвредность для окружающих.

Понятия безопасности законодатель привел в ст. 1***Закона о безопасности*,**где безопасность определяется как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз».

В ***Концепции национальной безопасности РФ***существенно дополнены и конкретизированы положения, ранее закрепленные в ***Законе о безопасности*.**

ВКонцепции введено понятие национальных интересов как со­вокупности сбалансированных интересов личности, общества и государства. При этом ограничен перечень областей, национальные интересы в которых определяют предмет национальной безопасно­сти: в области экономики, в социальной, внутриполитической, международной, информационной сферах, в области военной (обо­ронной), пограничной и экологической безопасности.

*Интересы личности*определены в Концепции как полное обеспечение конституционных прав и свобод, личной безопас­ности, повышение качества и уровня жизни, физическое, духов­ное и интеллектуальное развитие.

*Интересы общества*установ­лены в упрочении демократии, создании правового государства, достижении и поддержании общественного согласия, духовном обновлении России.

*Интересы государства*состоят в незыбле­мости конституционного строя, суверенитета и территориаль­ной целостности России, в политической, экономической и со­циальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии международного со­трудничества.

Таким образом, укрепление информационной безопасности названо в ***Концепции национальной безопасности РФ***в числе важнейших долгосрочных задач. Роль информационной безопас­ности и ее место в системе национальной безопасности страны определяется также тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое.

***В Доктрине информационной безопасности РФ***информа­ционная безопасность Российской Федерации определяется как состояние защищенности ее национальных интересов в информа­ционной сфере, определяющихся совокупностью сбалансирован­ных интересов личности, общества и государства.

В научной литературе в составе «информационной сферы об­щества» выделяют:

•     субъекты информационной сферы;

•     общественные отношения в информационной сфере;

•     информационную инфраструктуру общества;

•     информацию.

В соответствии с Законом обезопасности и содержанием Концепции национальной безопасности РФ под ***информацион­ной безопасностью***будем понимать состояние защищенности жиз­ненно важных интересов личности, общества и государства в информационной сфере.

Совокупность официальных взглядов на цели, задачи, прин­ципы и основные направления обеспечения информационной безопасности Российской Федерации представлена в Доктрине информационной безопасности РФ.

На основе анализа положений, содержащихся в доктринальных и нормативных правовых документах, можно выделить сле­дующие ***жизненно важные интересы в информационной сфере:***

•     *для личности:*

1.    соблюдение и реализация конституционных прав и свобод че­ловека и гражданина на поиск, получение, передачу, производст­во и распространение объективной информации;

2.    реализация права граждан на неприкосновенность частной жизни, защита информации, обеспечивающей личную безопас­ность;

3.    использование информации в интересах не запрещенной за­коном деятельности, физического, духовного и интеллектуально­го развития;

4.    защита права на объекты интеллектуальной собственности;

5.    обеспечение права граждан на защиту своего здоровья от не­осознаваемой человеком вредной информации;

•     *для общества:*

1.    обеспечение интересов личности в информационной сфере; построение правового социального государства;

2.    упрочение демократии, построение информационного обще­ства;

3.    духовное обновление общества, сохранение его нравственных ценностей, утверждение в обществе идеалов высокой нравствен­ности, патриотизма и гуманизма, развитие многовековых духов­ных традиций Отечества, пропаганда национального культурного наследия, норм морали и общественной нравственности; достижение и поддержание общественного согласия; предотвращение манипулирования массовым сознанием; приоритетное развитие современных телекоммуникационных технологий, сохранение и развитие отечественного научного и производственного потенциала;

•    *для государства:*

1.    создание условий для реализации интересов личности и обще­ства в информационной сфере и их защита;

2.    формирование институтов общественного контроля за орга­нами государственной власти;

3.    безусловное обеспечение законности и правопорядка; создание условий для гармоничного развития российской ин­формационной инфраструктуры;

4.    формирование системы подготовки, принятия и реализации решений органами государственной власти, обеспечивающей баланс интересов личности, общества и государства;

5.    защита государственных информационных систем и государ­ственных информационных ресурсов, в том числе государствен­ной тайны;

6.    защита единого информационного пространства страны; развитие равноправного и взаимовыгодного международного

7.    сотрудничества.

К ***основным задачам***в области обеспечения информационной безопасности относятся:

1.    формирование и реализация единой государственной полити­ки по обеспечению защиты национальных интересов от угроз в информационной сфере, реализации конституционных прав и свобод граждан в сфере информационной деятельности;

2.    разработка и создание механизмов формирования и реализа­ции государственной информационной политики России, в том числе разработка методов повышения эффективности участия

3.    государства в формировании информационной политики госу­дарственных телерадиовещательных организаций, других госу­дарственных средств массовой информации;

4.    совершенствование законодательства Российской Федерации в области обеспечения информационной безопасности;

5.    определение полномочий органов государственной власти Российской Федерации, субъектов Российской Федерации, орга­нов местного самоуправления и ответственности их должностных лиц, юридических лиц и граждан в области обеспечения инфор­мационной безопасности;

6.    развитие и совершенствование системы обеспечения инфор­мационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Россий­ской Федерации, а также системы противодействия этим угрозам; координация деятельности органов государственной власти по обеспечению информационной безопасности;

7.    совершенствование и защита отечественной информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с уче­том вхождения России в глобальную информационную инфра­структуру;

8.    проведение единой технической политики в области обеспе­чения информационной безопасности Российской Федерации; разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств; разви­тие стандартизации информационных систем на базе общепри­знанных международных стандартов и их внедрение для всех видов информационных систем;

9.    обеспечение технологической независимости Российской Фе­дерации, развитие отечественной индустрии телекоммуникацион­ных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

10. развитие научно-практических основ обеспечения информаци­онной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения «информационного оружия»;

11. разработка современных методов и средств защиты информа­ции, обеспечения безопасности информационных технологий, прежде всего, используемых в системах управления войсками и оружием, экологически опасными и экономически важными про­изводствами;

12. создание и развитие современной защищенной технологиче­ской основы управления государством в мирное время, в чрезвы­чайных ситуациях и в военное время;

13. защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти, на пред­приятиях оборонного комплекса, в том числе государственной тайны;

14. создание условий для успешного развития негосударственно­го компонента в сфере обеспечения информационной безопасно­сти, осуществления эффективного гражданского контроля за деятельностью органов государственной власти;

15. защиты культурного и исторического наследия (в том числе музейных, архивных, библиотечных фондов, основных историко-культурных объектов);

16. сохранение традиционных духовных ценностей при важней­шей роли Русской православной церкви и церквей других кон­фессий;

17. пропаганда средствами массовой информации элементов на­циональных культур народов России, духовно-нравственных, ис­торических традиций, норм общественной жизни и передового опыта подобной пропагандистской деятельности;

18. повышение роли русского языка как государственного языка и языка межгосударственного общения народов России и госу­дарств — участников СНГ;

19. создание оптимальных социально-экономических условий для осуществления важнейших видов творческой деятельности и фун­кционирования учреждений культуры;

20. противодействие угрозе развязывания противоборства в ин­формационной сфере;

21. создание единой системы подготовки кадров в области обес­печения информационной безопасности;

22. организация международного сотрудничества по обеспечению информационной безопасности при интеграции России в мировое информационное пространство на условиях равноправного парт­нерства.

Представляется, что юридическая наука в той или иной мере должна принимать участие в решении всех задач и реализации соответствующих целей, однако ее приоритет, решающая роль просматривается в двух областях:

-      во-первых, в определении разумного баланса между правом субъектов на свободное получение информации путем ее сбора или доступа к имеющимся ресурсам и правом субъектов на уста­новление ограничений в указанных действиях со стороны иных лиц по отношению к сведениям, обладателями которых они яв­ляются,

-      во-вторых, в разработке и реализации правовых мер защиты информации, доступ к которой должен ограничиваться по право­мерным основаниям, а также в обеспечении сохранности инфор­мационных ресурсов.

Для понимания проблемы определим еще два понятия: ***безопасность информации и защита информации****.*

Понятие *«безопасность информации»* распадается на две со­ставляющие:

-      безопасность  содержательной  части  (смысла)  информа­ции— отсутствие в ней побуждения человека к негатив­ным действиям, умышленно заложенных механизмов нега­тивного воздействия на человеческую психику или нега­тивного воздействия на иной блок информации (например, информация, содержащаяся в программе для ЭВМ, име­нуемой компьютерным вирусом);

-      защищенность информации от внешних воздействий (по­пыток   неправомерного   копирования,   распространения, модификации (изменения смысла) либо уничтожения.

Таким образом, защита информации входит составной частью в понятие безопасность информации.

Статьей 16 (ч. 1)ФЗ «Об информации, информационных технологиях и о защите информации» устанавливается следующее.

***Защита информации*** представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного дос­тупа, уничтожения, модифицирования, блокирования, копирова­ния, предоставления, распространения, а также от иных неправо­мерных действий в отношении такой информации;

2)  соблюдение конфиденциальности информации ограничен­ного доступа;

3) реализацию права на доступ к информации.

В этой связи можно выделить три основных направления правовой защиты объектов в информационной сфере (правового обеспечения информационной безопасности).

1.    ***Первое направление***. *Защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации* включает защиту:

-        чести, достоинства и деловой репутации граждан и организаций;

-        духовности и интеллектуального уровня развития личности;

-        нравственных и эстетических идеалов;

-        стабильности и устойчивого развития общества;

-        информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации.

(Институт массовой информации. Институт документированной информации. Нормы УК РФ. Нормы КоАП РФ).

2.    ***Второе направление****. Защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц* включает защиту:

-        информации и информационных ресурсов прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны);

-        информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц.

(Институт документированной информации. Институт государственной тайны. Институт коммерческой тайны. Институт персональных данных. Другие виды тайн. Нормы УК РФ. Нормы КоАП РФ. Нормы ГК РФ).

3.    ***Третье направление***. *Защита прав и свобод в информационной сфере в условиях информатизации включает* защиту:

-        права на производство, распространение, поиск, получение, передачу и использование информации;

-        права на интеллектуальную собственность;

-        права собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии.

(Институт интеллектуальной собственности. Институт документированной информации. Нормы УК РФ. Нормы КоАП РФ. Нормы ГК РФ).

## 2. Информация ограниченного доступа и ее защита

 С развитием информационного общества все большее значение приобретают проблемы, связанные с защитой информации ограниченного доступа.

Первая попытка определения понятия "конфиденциальная информация" была сделана в утратившем силу федеральном законе "Об информации, информатизации и защите информации", где в статье 2 к такой информации отнесена "документированная информация", доступ к которой ограничивается в соответствии с законодательством Российской Федерации". А в соответствии со ст.10 "документированная информация с ограниченным доступом ....подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную".  В новом законе «Об информации, информационных технологиях и о защите информации» понятия «информация ограниченного доступа» или «конфиденциальная информация» вообще не определены.

В отсутствие специальных законов единственным документом, определяющим структуру  конфиденциальной информации, является Указ Президента РФ №188 от 6 марта 1997 года. Указом к сведениям конфиденциального характера отнесены:

-        сведения о частной жизни гражданина (персональные данные), позволяющие идентифицировать его личность;

-        сведения, составляющие тайну следствия и судопроизводства; служебная тайна;

-        сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная  адвокатская тайна, тайна переписки, телефонных разговоров и т.д.);

-        коммерческая тайна;

-        информация об изобретениях и новых технологиях (до официальной публикации информации о них).

Федеральные законы «О коммерческой тайне» и «О персональных данных» также содержат положения о видах и формах информации ограниченного доступа  в регулируемых областях.

Согласно ч.2 ст. 5 ФЗ «Об информации, информационных технологиях и о защите информации» информация ***в зависимости от категории доступа*** к ней подразделяется на *общедоступную* информацию, а также на информацию, доступ к которой ограничен федеральными законами (*информация ограниченного доступа*).

К ***общедоступной информации*** относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Она может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации (ст.7).

***Ограничение доступа*** к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (ч.1 ст. 9).

С точки зрения этимологии, слово «конфиденциальный» происходит от латинского confidentia - доверие и в современном русском языке означает «доверительный, не подлежащий огласке, секретный». Слово «секрет», которое также необходимо рассмотреть, заимствовано из французского secret – «тайна». Интересно, что в знаменитом словаре В. Даля также названы аналогичные значения: «конфиденциальная» - «откровенная, по особой доверенности, неоглашаемая, задушевная»; «тайна» - «кто чего не знает, то для него тайна, все сокрытое, неизвестное, неведомое». Таким образом, можно сделать вывод о равнозначности понятий информация ограниченного доступа, конфиденциальная информация, тайна и секрет.

Однако, как отмечает А.А. Ефремов, понятие тайны в правовой науке не совсем совпадает с понятием конфиденциальной информации, так как тайна означает ещё и правовой режим информации. Как отмечает А. И. Алексенцев, понятия «секретный», «конфиденциальный», «тайна» равнозначны. Таким образом, как правильно указал А. И. Алексенцев к конфиденциальной информации должна быть отнесена вся информация с ограниченным доступом, составляющая любой вид тайны.

В настоящее время нет четкой и единой классификации видов информации ограниченного доступа, хотя действующими нормативными актами установлено свыше 30 ее разновидностей. Определенные попытки такой классификации предприняты учеными. А. И. Алексенцев предлагает следующие ***основания разделения информации по видам тайны***:

-      собственники информации (по отдельным видам они могут частично совпадать);

-      области (сферы) деятельности, в которых может быть информация, составляющая данный вид тайны;

-      на кого возложена защита данного вида тайны (по некоторым видам тайны здесь также возможно совпадение).

А. А. Фатьянов ***классифицирует***подлежащую защите информацию по трем признакам: по принадлежности, по степени конфиденциальности (степени ограничения доступа) и по содержанию.

*По принадлежности* владельцами защищаемой информации могут быть органы государственной власти и образуемые ими структуры (государственная тайна, служебная тайна, в определенных случаях коммерческая и банковская тайны); юридические лица (коммерческая, банковская служебная, адвокатская, врачебная, аудиторская тайны и т.п.); граждане (физические лица) - в отношении личной и семейной тайны, нотариальной, адвокатской, врачебной.

*По степени конфиденциальности* (степени ограничения доступа) в настоящее время можно классифицировать только информацию, составляющую государственную тайну. Согласно ст.8 Закона РФ «О государственной тайне», устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений : «особой важности», «совершенно секретно» и «секретно». Интересно, что в США и ряде стран НАТО грифы секретности схожи с установленными отечественным законодательством – «конфиденциально (confidential)», «секретно (secret)», «совершенно секретно (top secret)». Для остальных видов тайн данное основание классификации пока не разработано, при этом согласно ст. 8 Закона РФ «О государственной тайне», использование названных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

*По содержанию* защищаемая информация может быть разделена на политическую, экономическую, военную, научную, технологическую, личную, коммерческую и т.п.

Следует отметить, что вышеизложенные классификации не являются исчерпывающими и их разработка еще предстоит науке и законодательству.

В ст.9 ФЗ «Об информации, информационных технологиях и о защите информации» выделяют следующие виды информации ограниченного доступа:

1)    государственную тайну,

2)    коммерческую тайну,

3)    информацию о частной жизни лица (персональные данные, личную или семейную тайну),

4)    профессиональную тайну,

5)    служебную тайну и иную тайну.

***Защита государственной тайны*** осуществляется на основе  Закона   РФ  от 21 июля 1993 г. № 5485-1 « О   государственной   тайне» в статье 3 которого указывается:  *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.

***Защита коммерческой тайны*** осуществляется на основе ФЗ  от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне», в статье 3 которого указывается:

1) *коммерческая тайна* - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

2) *информация, составляющая коммерческую тайну*, - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

3) *режим коммерческой тайны* - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

***Защита персональных данных*** осуществляется на основе ФЗ от 27 июля 2006 г. N 152-ФЗ «О персональных данных», в статье 3 которого указывается: *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.

***Профессиональная тайна*** – конфиденциальная информация, защищаемая по закону, не являющаяся государственной тайной и доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения.

К *объектам* профессиональной тайны относится: врачебная аудиторская, нотариальная, журналистская (редакционная), адвокатская тайна, тайна связи, усыновления, страхования, исповеди.

***Служебная тайна*** – конфиденциальная информация, защищаемая по закону и  не являющаяся государственной тайной, ставшая известной в органах государственной власти и органах местного самоуправления на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом.

К *объектам* служебной тайны относится: военная, судебная, налоговая, банковская тайна и тайна следствия.

## 3. Принципы, методы и  средства системы защиты информации

Организационные мероприятия и процедуры, используемые для решения проблемы безопасности информации, решаются на всех этапах проектирования и в процессе эксплуатации ИС.

Создание ***базовой системы защиты информации*** в ИС  основывается на следующих ***принципах***;

1.    *Комплексный подход* к построению системы защиты при ведущей роли организационных мероприятий, означающий оптимальное сочетание программно-аппаратных средств и организационных мер защиты.

2.    *Разделение и минимизация полномочий* по доступу к обрабатываемой информации и процедурам обработки, т.е.  предоставление  пользователям минимума строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автономной обработки доступной им конфиденциальной информации.

3.    *Полнота контроля и регистрация* попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и  протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ИС без ее предварительной регистрации.

4.    *Обеспечение надежности системы защиты*, т.е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей или обслуживающего персонала.

5.    *Обеспечение контроля за функционированием системы защиты*, т.е. создание средств и методов контроля работоспособности механизмов защиты.

6.    *Экономическая целесообразность* использования системы защиты, выражающаяся в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации ИС без системы защиты информации.

При реализации перечисленных принципов в практической деятельности используются следующие ***методы*** обеспечения безопасности информации.

*Препятствие*– метод физического преграждения путем злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).

*Управление доступом* – метод защиты информации регулированием использования всех ресурсов ИС, включает следующие функции защиты:

а) идентификацию пользователей, персонала и ресурсов системы;

б) опознание объекта или субъекта по предъявленному им идентификатору;

в) проверку полномочий;

г) разрешение и создание условий работы в пределах установленного регламента;

д) регистрацию обращений к защищаемым ресурсам;

е) регулирование при попытках несанкционированных действий (сигнализация, отключение, задержка работ, отказ в запросе).

*Маскировка*– метод защиты информации путем ее криптографического закрытия. При передаче информации по каналам связи большой  протяженности этот метод является единственно надежным.

*Регламентация* – метод защиты информации создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

*Принуждение* – метод защиты информации, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или  уголовной ответственности.

*Побуждение* – метод защиты информации, который побуждает  пользователей ИС не разрушать  установленные порядки за счет соблюдения сложившихся моральных и этических норм, как регламентированных, так и неписаных.

Рассмотренные методы обеспечения безопасности информации реализуются на практике за счет  применения различных ***средств***защиты.

*Технические средства* реализуются в виде  электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу (устройства для сканирования отпечатков пальцев, сетчатки глаза и т.п.).

Физические средства реализуются в виде автономных устройств и систем (замки, решетки, электромеханическое оборудование  охранной  сигнализации).

*Программные средства* представляют ПО, специально предназначенное для выполнения функций защиты информации.

*Организационные средства* защиты представляю собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Эти мероприятия охватывают все структурные  элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование ИС, монтаж и наладка оборудования, испытания, эксплуатация).

*Законодательные средства* определяются законодательными актами страны, которыми  регламентируются правила  пользования, обработки и передачи информации  ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

*Морально-этические средства* защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения ВТ и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека.

Все рассмотренные средства защиты разделены на *формальные*, которые выполняют защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека, и  *неформальные*, которые определяются целенаправленной деятельностью человека либо регламентируют эту деятельность.

## 4. Основные направления и виды защиты информации

Виды защиты в информационных системах классифицируются по направлениям защиты. К *основным направлениям защиты* относятся:

- защита информации от несанкционированного доступа;

- защита информации в системах связи;

- защита юридической значимости электронных документов;

- защита конфиденциальной информации от утечки по кана­лам побочных электромагнитных излучений и наводок;

- защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;

-  защита от несанкционированного копирования и распростра­нения программ и ценной компьютерной информации.

С точки зрения защиты информации *несанкционированный доступ* может иметь следую­щие *последствия*: утечка обрабатываемой конфиденциальной ин­формации, а также ее искажение или разрушение в результате умышленного нарушения работоспособности ИТ.

*Видами защиты информации от несанкцио­нированного доступа* являются

1)    разграничение полномочий и доступа к информации;

2)    регистрация, при которой фиксируются все осуществленные или неосуществлен­ные попытки доступа к данным или программам.

Система регистрации и учета осуществляет:

- регистрацию входа (выхода) субъектов доступа в систему (из системы) либо регистрацию загрузки и инициализации операцион­ной системы и ее программного останова;

- регистрацию и учет выдачи печатных (графических) докумен­тов на твердую копию;

- регистрацию запуска (завершения) программ и процессов (за­даний, задач), предназначенных для обработки защищаемых фай­лов;

- регистрацию попыток доступа программных средств к защищаемым файлам;

-  учет всех защищаемых носителей информации.

К видам защиты информации в *системах связи* относятся применение криптографии и специальных связных протоколов.

К видам защиты *юридической значимости электронных документов* относится применение «цифровой подписи», которая является одним из криптографических методов проверки подлинности ин­формационных объектов.

Для защиты *от побочных электромагнит­ных излучений и наводок* применяется экранирование по­мещений, предназначенных для размещения средств вычислитель­ной техники, а также технические меры, позволяющие снизить ин­тенсивность информативных излучений ПЭВМ и средств  связи.

Видами защиты информации от *компьютерных вирусов* и других опас­ных воздействий по каналам распространения программ являются:

- «иммуностойкие» программные средства, за­щищенные от возможности несанкционированной модифика­ции (разграничение доступа, методы самоконтроля и самовос­становления);

- специальные программы-анализаторы, осущест­вляющие постоян­ный контроль возникновения отклонений в работе прикладных программ, периодическую проверку нали­чия других возможных следов вирусной активности, а также входной контроль новых программ перед их использованием.

Защита от *несанкционированного копирования и распростране­ния программ и ценной компьютерной информации* осуществляется с помощью специальных программ­ных средств, подвергающих защищаемые программы и базы дан­ных предварительной обработке (вставка парольной защиты, про­верки по обращению к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабо­чей ПЭВМ по ее уникальным характеристикам и т.д.), которая приводит исполняемый код защищаемой программы и базы данных в состояние, препятствующее его выполнению на «чужих» машинах.

Контроль целостности программного обеспечения проводится с помощью внешних средств (программ контроля целостности) и с помощью внутренних средств (встроенных в саму программу). Внешние средства осуществляют контроль при старте системы, а также при каждом запуске программы на выполнение. Внутренние средства контролируют вы­полнение программ при каждом запуске на выполнение и состоят в сравнении контрольных сумм отдельных блоков программ с их эталонными суммами.

Противодействие несанкционированному изменению прикладных и специальных программ можно обеспечить разными способами, в частности методом контроля целостности базового программного обеспечения спе­циальными программами.

При защите коммерческой информации поль­зуются всей совокупностью  существующих средств и систем защиты данных. Однако при их выборе следует исходить из сравнительной оценки важности защищаемой информации и ущерба, который может нанести ее утрата.

Из перечисленных средств защиты наиболее надежными и эффективными являются системы и средства, построенные на базе криптографических методов.

**Задания:**

1. **Прочитать и законспектировать основные моменты лекции.**
2. **Ответить на контрольные вопросы письменно:**
3. Проанализируйте состояние информационной безопасности в кабинете информатики нашего учебного заведения. Предложите дополнительные мероприятия по повышению уровня информационной безопасности.
4. Приведите примеры из жизни, из кино- и видеофильмов, иллюстрирующие использование уязвимых мест и нарушения мер защиты информационной безопасности для несанкционированного проникновения в охраняемые системы.

***Примечание****:*

*Задание выполнить в рабочих тетрадях, фото или сканы листов отправить до 17.00 25.03.2020 на электронную почту преподавателя* ***aigulanvarovna@gmail.com*** *в теме письма указав номер группы и фамилию студента*