Тема 1. Основные понятия курса «Информационная безопасность»

1. Основные понятия и определения ИБ

Современный этап информатизации связан с использованием персональной вычислительной техники, систем телекоммуникаций, развитием компьютерных сетей. Возрастает потребность в разработке и применении эффективных решений в сфере информационной индустрии.
На определенном этапе развития информационной индустрии рождается информационное общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, т.е. творческим трудом, направленным на развитие интеллекта и получение знаний. Создается единое, не разделенное национальными границами информационное сообщество.

Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена.

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин *"информационная безопасность"* используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Под ***информационной безопасностью*** мы будем понимать защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*. (Чуть дальше мы поясним, что следует понимать под *поддерживающей инфраструктурой*..

Таким образом, правильный с методологической точки зрения подход к проблемам *информационной безопасности* начинается с выявления *субъектов информационных отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Чтобы понять, от чего нужно защищать информацию, необходимо ввести понятие **угрозы** – возможного происшествия (преднамеренного или нет), которое способно оказать нежелательное воздействие на активы и ресурсы, связанные с вычислительной системой. Принято выделять три различных типа угроз, и соответственно, три свойства информации: конфиденциальность, целостность и доступность.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (согласно ФЗ-149 «Об информации, информационных технологиях и о защите информации»);

Конфиденциальность — обеспечение доступа к информации только авторизованным пользователям

Целостность — обеспечение достоверности и полноты информации и методов ее обработки. (ГОСТ Р ИСО/МЭК 17799-2005, ст. 2.1).

Целостность информации — состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право (Р 50.1.056-2005, ст. 3.1.6).

Доступность — обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Угроза раскрытия заключается в том, что информация становится известна неавторизованному пользователю. Она возникает всякий раз, когда получен несанкционированный доступ к секретной информации, хранящейся в вычислительной системе, или передаваемой от одной системы к другой. Иногда в связи с угрозой информации используется термин «утечка информации»

Угроза целостности включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую

Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий умышленно блокируется доступ к некоторому ресурсу вычислительной системы

Контролируемая зона — территория вокруг предприятия, на которой исключено неконтролируемое пребывание посторонних лиц и любого вида транспорта, не имеющих постоянного или разового пропуска на эту территорию.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Несанкционированный доступ (НСД) к информации – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС, преднамеренное обращение субъекта к компьютерной информации, доступ к которой ему не разрешен, независимо от цели обращения.

Администратор АС – физическое лицо, ответственное за функционирование АС в установленном штатном режиме работы.

Администратор безопасности – физическое лицо, ответственное за защиту АС от НСД к информации.

Информация, составляющая коммерческую тайну – информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Режим разграничения доступа – порядок доступа к компьютерной информации в соответствии с установленными правилами.

Защита информации – это деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Виды защиты информации (согласно ГОСТ Р 50922-2006)

- **правовая защита информации:** разработка законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.
- **криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования.
- **техническая защита информации:** обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств.
- **физическая защита информации:** путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Основные цели ЗИ:

1. Соблюдение конфиденциальности информации ограниченного доступа.
2. Предотвращение НСД к информации и (или) передачи её лицам, не имеющим права на доступ к такой информации.
3. Предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию и предоставлению информации, а также иных неправомерных действий в отношении такой информации.
4. Реализация конституционного права граждан на доступ к информации
5. Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование

2. Классификация угроз информационной безопасности

Под **угрозой** обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку – **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

В дальнейшем **угрозой ИБ** АС будем называть возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

В настоящее время рассматривается достаточно обширный перечень угроз ИБ АС, насчитывающий сотни пунктов. Наиболее характерные и часто реализуемые из них перечислены ниже:

- несанкционированное копирование с носителей информации;
- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
- игнорирование установленных правил при определении ранга системы.

Необходимость классификации угроз ИБ АС обусловлена тем, что архитектура современных средств автоматизированной обработки информации, организационное, структурное и функциональное построение информационно-вычислительных систем и сетей, технологии и условия автоматизированной обработки информации такие, что накапливаемая, хранимая и обрабатываемая *информация подвержена случайным влияниям чрезвычайно большого числа факторов*, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Как следствие, для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз.

Классификация всех возможных угроз ИБ АС может быть проведена по ряду базовых признаков.

1. **По природе возникновения:**
   - естественные угрозы – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека;
   - искусственные угрозы – угрозы ИБ АС, вызванные деятельностью человека.
2. **По степени преднамеренности проявления**:

2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала:

- проявление ошибок программно-аппаратных средств АС;
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи;

2.2. Угрозы преднамеренного действия (например, угрозы действий злоумышленника для хищения информации);

3. **По непосредственному источнику угроз**:

3.1. Угрозы непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение);

3.2. Угрозы непосредственным источником которых является человек:

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
- вербовка (путем подкупа, шантажа) персонала или отдельных пользователей, имеющих определенные полномочия;
- угроза несанкционированного копирования секретных данных пользователем АС;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков);

3.3. Угрозы непосредственным источником которых являются санкционированные программно-аппаратные средства:

- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных);
- возникновение отказа в работе операционной системы;

3.4. Угрозы непосредственным источником, которых являются несанкционированные программно-аппаратные средства:

- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических, не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами с деструктивными функциями;

4. **По положению источника угроз**:

4.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС:

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания и отопления);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- дистанционная фото и видеосъемка;

4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС:

- хищение производственных отходов (распечаток, записей, списанных носителей информации);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи);
- применение подслушивающих устройств;

4.3. Угрозы, источник которых имеет доступ к периферийным устройствам АС;

4.4. Угрозы, источник которых расположен в АС:

- проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;
- некорректное использование ресурсов АС;

5. **По степени зависимости от активности АС**:

5.1. Угрозы, которые могут проявляться независимо от активности АС:

- вскрытие шифров криптозащиты информации;
- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем);

5.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных (например, угрозы выполнения и распространения программных вирусов);

6. **По степени воздействия на АС:**

6.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (например, угроза копирования секретных данных);

6.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС:

- внедрение аппаратных спец вложений, программных «закладок» и «вирусов» («троянских коней» и «жучков»), т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют

преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы);
- угроза умышленной модификации информации;

7. **По этапам доступа пользователей или программ к ресурсам АС**:

- угрозы, которые могут проявляться на этапе доступа к ресурсам АС (например, угрозы несанкционированного доступа в АС);
- угрозы, которые могут проявляться после разрешения доступа к ресурсам АС (например, угрозы несанкционированного или некорректного использования ресурсов АС);

8. **По способу доступа к ресурсам АС:**

8.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС:

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики.

8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС:

- вход в систему в обход средств защиты (загрузка посторонней ОС со сменных магнитных носителей);
- угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС;

9. **По текущему месту расположения информации, хранимой и обрабатываемой в АС:**

9.1. Угрозы доступа к информации на внешних запоминающих устройствах (например, угроза несанкционированного копирования секретной информации с жесткого диска);

9.2. Угрозы доступа к информации в оперативной памяти:

- чтение остаточной информации из оперативной памяти;
- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;
- угроза доступа к системной области оперативной памяти со стороны прикладных программ;

9.3. Угрозы доступа к информации, циркулирующей в линиях связи:

- незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;
- перехват всего потока данных с целью дальнейшего анализа не в реальном масштабе времени;

9.4. Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере (например, угроза записи отображаемой информации на скрытую видеокамеру).

Модель угроз информационной безопасности – это описание существующих угроз ИБ, их актуальности, возможности реализации и последствий.

3. Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

- В **Доктрине информационной безопасности Российской Федерации** (здесь, подчеркнем, термин *"информационная безопасность"* используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.
- По распоряжению президента США Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью *информационного оружия*. В начале октября 1997 года при подготовке доклада президенту глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.
- Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (*Government* Computer News, июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию

коммерческого программного обеспечения с целью снижения стоимости военной техники.

- Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).
- Как сообщил журнал Internet Week от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от **компьютерных преступлений** достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.
- В середине июля 1997 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару.
- В феврале 2001 года двое бывших сотрудников компании *Commerce* One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.
- Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи – недостатка в нарушениях *ИБ* нет и не предвидится. Чего стоит одна только "Проблема 2000" – стыд и позор программистского сообщества!

При анализе проблематики, связанной с *информационной безопасностью*, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что *информационная безопасность* есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько *механизмы* генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения *ИБ*. Следует исходить из того, что необходимо конструировать надежные системы (*информационной безопасности*) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении **жизненного цикла ИС**.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый *по* счету, годовой отчет "Компьютерная преступность и *безопасность*-1999: проблемы и тенденции" (*Issues and Trends*: 1999 *CSI*/*FBI Computer Crime and Security* Survey). В отчете отмечается резкий рост числа обращений в правоохранительные органы *по* поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их *информационные системы* были взломаны внешними злоумышленниками; атакам через *Internet* подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?" ответили "не знаю".

В аналогичном отчете, опубликованном в апреле 2002 года, цифры изменились, но тенденция осталась прежней: 90% респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели *место* нарушения информационной безопасности; 80% констатировали финансовые потери от этих нарушений; 44% (223 респондента) смогли и/или захотели оценить потери количественно, общая сумма составила более 455 млн. долларов. Наибольший *ущерб* нанесли кражи и *подлоги* (более 170 и 115 млн. долларов соответственно).

Столь же тревожные результаты содержатся в обзоре InformationWeek, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об отсутствии нарушений *информационной безопасности*. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак – еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США (National *Infrastructure Protection Center*, *NIPC*) от 21 июля 1999 года сообщается, что за период с 3 *по* 16 июля 1999 года выявлено девять проблем с *ПО*, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди "пострадавших" операционных платформ – почти все разновидности ОС

Unix, *Windows*, MacOS, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы *информационной безопасности* должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная *активность* практически незаметна. Целью злоумышленников может быть нарушение всех составляющих *ИБ* – доступности, целостности или конфиденциальности

4. Информационные войны и информационное оружие.

Информационная война — информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство — форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность (киберпреступность) — проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях.

Особенности: объектом воздействия являются все виды информации и информационных систем; информация может выступать и как оружие, и как объект защиты; территория и производство ведения войны осуществляется на неограниченном пространстве; информационная война ведется как при объявлении войны, так и просто в кризисных ситуациях; ведется как военными, так и гражданскими структурами.

Концепция информационной войны: силовой технический метод – подавление элементов инфраструктуры государственного управления; радиоэлектронная борьба – электромагнитное воздействие; хакерная война; формирование и массовое распространение по информационным каналам противника или глобальным сетям; получение интернациональной информации путем перехвата и обработки открытой информации.

Способы защиты:

1. информация в Internet подлежит защите с помощью криптозащиты, т. е. шифрование;
2. меры административного и технического характера: установление блокиратора; контроль доступа; проверка поставщика программы.

Информационное оружие – средство уничтожения, искажения или хищения информационных массивов, добывание из них необходимой информации после преодоления систем защиты.

Отличительные черты информационного оружия: скрытность; масштабность; универсальность.

Виды: обычное; высокоинтеллектуальное (самонаводящее); радиочастотные, маскирующие помехи; сильное излучение; воздействие систем связи на ЭВМ; средства генерации естественной речи конкретного человека.

Важным свойством информационного оружия является его поражающее свойство. Это поражающее свойство информационного оружия направлено на человека. Особо опасным является воздействие, которое осуществляется на мозг человека, при этом происходит трансформирование матрицы (памяти) – искусственная амнезия.

Подобные изменения могут осуществляться программными закладками, например «25 кадр».

Защита от подобного вторжения в психическую деятельность человека осуществляется следующими способами:

- воспитание;
- эстетические фильтры;
- создание общественной защиты.

Используя результаты исследования в области информационной безопасности, законодатель и исследователи отрасли информационного права приобретают дополнительные возможности совершенствования средств и механизмов правовой защиты информационной безопасности в информационной сфере. Таким образом, существенно повышаются качество и эффективность правового регулирования отношений в информационной сфере.

Основные направления защиты информационной сферы:

1. защита интересов личности, общества, государства от воздействия вредной, опасной, недоброкачественной информации;
2. защита информации, информационных ресурсов и информационных систем от неправомерного воздействия посторонних лиц;
3. защита информационных прав и свобод.

Правовые механизмы защиты жизненно важных интересов личности, общества, государства должны разрабатываться в каждой из областей информационной сферы.