**Тема 4. Правовое регулирование информационной безопасности.**

***Сущность информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Информационная безопасность личности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации. Перспективы развития законодательства в области информационной безопасности.***

**4.1. Сущность информационной безопасности.**

Рассмотрим несколько определений информационной безопасности (ИБ).

1. **ИБ** – это комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех атворизованных пользователей.

2. **ИБ** – показатель, отражающий статус защищенности информационной системы и информационной среды.

3. **ИБ** – состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.

4. **ИБ** – состояние защищенности информационных ресурсов, технологии их формирования и использования, а также правового статуса субъектов информационной деятельности.

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

Внутри ИБ можно выделить 3 сферы:

1. Угроза информационным правам и свободам личности, общества и государства.

2. Угроза воздействия некачественной или ложной информации (дезинформации).

3. Угроза несанкционированного неправомерного воздействия посторонних лиц на информацию.

**Объектом ИБ** является то, что защищается от угроз (граждане, общество, государство, но прежде всего это информационные ресурсы, содержащие данные.

Опасности и угрозы всегда указывают на взаимодействие 2 сторон:

Субъекта – источника и носителя опасности;

Объекта – на которого направлена опасность или угроза.

Различают следующие виды причин угроз ИБ:

1. **Случайные угрозы** – вызванные авариями, сбоями, ошибками разработчиков и персонала.
2. **Преднамеренные угрозы,** вызванные злоумышленными действиями людей.
3. Угрозы, направлены на нарушение основных свойств информации: конфиденциальности, целостности, доступности информации.

В Доктрине информационной безопасности РФ источники угроз делятся на 2 группы:

I. **Внешние угрозы** деятельность иностранных структур.

II. **Внутренние угрозы** представляют собой неразвитость правовой базы, коррупцию и т.д.

**Информационная безопасность личности** включает следующие факторы:

– состояние защищённости, при котором отсутствует угроза причинения вреда информации, которой владеет личность;

– состояние и условие жизнедеятельности личности, при которых отсутствует угроза нанесения вреда личности информацией.

**Интересы личности в информационной сфере** заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления : запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

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

**Интересы государства в информационной сфере** заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользованияею 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.

**Система обеспечения информационной безопасности РФ** является частью системы обеспечения национальной безопасности страны. Система обеспечения информационной безопасности РФ строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

**Угрозы информационной безопасности Российской Федерации**:

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

– угрозы информационному обеспечению государственной политики Российской Федерации;

– 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;

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

**4.2. Субъекты и объекты правоотношений в области информационной безопасности.**

К объектам в области создания и применения информационных систем, информационных технологий и средств их обеспечения относятся: информационные системы и информационные технологи, средства их обеспечения.

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

**Средства обеспечения автоматизированных информационных систем и их технологий** – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатации.

К информационным системам относятся и автоматизированные информационные системы разного вида. В первую очередь это Интернет, а также автоматизированные системы управления (АСУ), автоматизированные системы обработки данных (АСОД), автоматизированные системы научно-технической информации (АСНТИ) и т. п., банки данных, базы знаний, экспертные системы, информационно-вычислительные системы, информационно-телекоммуникационные системы и сети, системы связи и телекоммуникации, а также средства обеспечения этих систем и технологий.

**Основные технические средства** – средства вычислительной техники, копировально-множительная техника, оргтехника, средства связи и телекоммуникаций и др.

**Программные средства** – операционные системы, прикладные программы, программные средства телекоммуникации, другие программные средства.

**Лингвистические средства** – словари, тезаурусы, классификаторы, другие лингвистические средства, организационно-правовые средства – нормативные правовые и правовые акты, нормативно-технические документы, положения, уставы, должностные инструкции.

Субъектов в области информационных технологий и средств их обеспечения можно разделить на две группы:

– субъекты, организующие и осуществляющие разработку информационных систем, информационных технологий и средств их обеспечения;

– субъекты, эксплуатирующие перечисленные объекты.

В качестве субъектов, организующих и выполняющих разработку информационных систем, выступают заказчики и разработчики. Это – органы государственной власти, юридические и физические лица – организации и предприятия, специалисты. Субъектами, эксплуатирующими информационные системы, информационные технологии, являются органы государственной власти, их подразделения, юридические и физические лица.

Одним из важнейших направлений деятельности субъектов в этой области должны быть формирование и развитие программно-технической части информационной инфраструктуры современного информационного общества.

**Информационная инфраструктура** – организованная совокупность средств вычислительной техники, связи и телекоммуникаций, а также массовой информации и информационных ресурсов, обеспечивающая эффективную и качественную реализацию информационных процессов - процессов производства, сбора, накопления, хранения, поиска, распространения и потребления информации для удовлетворения потребностей личности, общества, государства.

**База данных (БД)** – организованная в соответствии с определёнными правилами и поддерживаемая в памяти компьютера совокупность данных, характеризующая актуальное состояние некоторой [предметной области](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BC%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D1%8C) и используемая для удовлетворения информационных [потребностей](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BD%D0%BE%D1%81%D1%82%D1%8C) пользователей. Она должна отражать текущие данные о предметной области, накапливать, хранить информацию и предоставлять различным категориям пользователей быстрый доступ к данным.

По характеру хранимой информации БД делятся на фактографические и документальные. В **фактографических БД** содержатся краткие сведения об описываемых объектах, представленные в строго определенном формате. Например, каталог в библиотеке. В **документальных БД** содержится информация самого разного типа: текстовая, графическая, звуковая. Например, БД законодательных актов в области уголовного права.

Сама база данных включает в себя только информацию. Информационная система представляет собой совокупность базы данных и комплекса аппаратно-программных средств сбора, хранения, передачи и обработки информации. ИС условно можно также разделить на фактографические и документальные. Фактографические ИС выполняют функции обработки БД.

4.3. **Информационная безопасность личности.**

Угрозами информационной безопасности личности являются следующие:

– принятие нормативных актов, противоречащих конституционным правам граждан;

– противодействие реализации гражданами прав на неприкосновенность частной жизни;

– неправомерное ограничение доступа к открытой информации;

– нарушение прав граждан в области массовой информации.

– противоправное применение специальных средств, воздействующих на сознание человека;

– манипулирование информацией.

Источниками угроз информационной безопасности личности также могут выступать другая личность, программные и технические средства, группа лиц, общественная группа или даже государство, интернет, СМИ и др.

Законодательство РФ сегодня не в полной мере обеспечивает безопасность личности в информационной сфере. В таких условиях наиболее незащищенными являются дети и подростки, молодежь, еще не выработавшая строгого мировоззрения, четкую жизненную позицию. Поэтому проблема информационной безопасности личности приобретает особую значимость в контексте социально-педагогической деятельности. Так как целью практической социально-педагогической деятельности является гармонизация взаимодействия (отношений) личности и социума для сохранения, восстановления, поддержания, развития социальной активности этого человека. В условиях, когда не учитывается информационный аспект, построить гармоничное взаимодействие личности и социума вряд ли удастся.

По общему мнению, решение проблемы обеспечения информационной безопасности личности, должно носить комплексный системный характер и осуществляться на разных уровнях.

Первый уровень – нормативный. На данном уровне органы государственной власти должны создать непротиворечивую нормативную базу, учитывающую все аспекты проблемы информационной безопасности.

Второй уровень – институциональный, включает в себя согласованную деятельность различных социальных институтов, связанных с воспитанием и социализацией, по обеспечению информационной безопасности личности. В первую очередь к таким институтам относятся семья, школа для детей и подростков, церковь.

Третий уровень – личностный. Этот уровень связан, прежде всего, с самовоспитанием, самообразованием, формированием высокого уровня информационной культуры личности как части общей культуры человека. На данном уровне происходит формирование необходимых личностных качеств для обеспечения информационной самозащиты личности.

В настоящее время можно выделить следующие наиболее существенные формы информационно-технических опасностей, обусловленных достижениями научно-технического прогресса в условиях глобализации:

– первая форма связана с бурным развитием нового класса оружия – информационного, которое способно эффективно воздействовать и на психику, сознание людей, и на информационно-техническую инфраструктуру общества и армии.

– вторая форма связана с использованием современных информационных технологий (махинации с электронными деньгами, компьютерное хулиганство и др.).

– третья форма связана с использованием современных информационных технологий в политических целях.

Сегодня источниками права в сфере информационной безопасности личности являются следующие:

– Конституция РФ;

– Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895);

– Указ Президента РФ от 12 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

**4.4. Система нормативных правовых актов (источников права), регулирующих обеспечение информационной безопасности в Российской Федерации.**

* нормативные акты в области информации;
* нормативные акты в области защиты информации;
* международные акты.

**Информационное законодательство** представляет собой совокупность законов, иных нормативно-правовых актов, с помощью и посредствам которых государство устанавливает, изменяет либо прекращает действие соответствующих информационно-правовых норм. Информационное законодательство выступает главенствующей формой закрепления норм информационного права и важнейшим правообразующим фактором. Появление информационного законодательства в системе нормативно-правовых актов РФ свидетельствует о повышении роли государства в регулировании информационных отношений и придании им качества общественно значимых отношений.

Систему информационного законодательства образуют различные законы и издаваемые в соответствии с ними иные нормативные правовые акты, посвященные прямому или опосредованному регулированию отношений, объектом которых является информация, производные от нее продукты и связанная с ними деятельность.

Системы информационного законодательства включает в себя правовые акты федеральных органов и органов субъектов РФ.  
Среди правовых актов федеральных органов главное место занимают федеральные законы. Они обладают высшей юридической силой, регулируют наиболее важные, основополагающие отношения и содержат информационно-правовые нормы исходного характера, которые рассчитаны на постоянное либо длительное действие.

Нормативные акты, не относящиеся к категории законов, являются подзаконными. В их число входят нормативные акты Президента РФ, Правительства РФ, ведомственные нормативные акты.

Многие из них носят комплексный характер, но включают в себя и правила информационно-правового содержания.

**Указы Президента РФ** – основные акты осуществления компетенции Президента РФ, непосредственно закрепленной в Конституции РФ и вытекающей из основополагающих принципов разделения властей. Правовые акты Правительства РФ издаются главным образом тогда, когда в законе есть на то прямые указания либо дано конкретное поручение Президента РФ.

Ведомственные акты издаются на основе законов, указов президента и актов правительства. Они представляют собой управленческие акты органов специальной компетенции. Их юридическая сила зависит от функций издавшего их органа и специфики государственного управления информационной сферой. На уровне субъектов РФ применяются все те же формы выражения информационного права, что и на федеральном уровне (законы субъектов РФ, постановления органов исполнительной власти, акты отраслевых и территориальных органов управления).

Наряду с актами законодательства и подзаконными нормативными актами существуют так называемые локальные нормативные акты Они, как правило, представляют собой приказы и распоряжения нормативного и индивидуального значения, принимаемые руководителями различных организаций. С помощью локальных актов регулируются самые различные информационные вопросы, например, порядок конфиденциального делопроизводства, допуска сотрудников к служебной и коммерческой тайнам, порядок организации защиты коммерческой тайны в организации и т. п.

В систему информационного законодательства следует включить и международно-правовые акты, предметом регулирования которых являются информационные отношения.

Несмотря на то, что информационное законодательство находится на этапе своего становления, уже сегодня можно говорить о наличии некой его упорядоченности. В основу этой упорядоченности положен принцип иерархии, выражающийся в соподчиненности актов различного уровня. Первый уровень, который можно условно назвать конституционным, отражает ведущую роль Конституции в информационно-правовом нормотворчестве. Он представлен рядом конституционных норм. Второй уровень нормативных правовых актов составляют акты информационного законодательства. Специфика данного уровня состоит в том, что федеральные законы, регулирующие отношения в информационной среде, а равно иные принятые в соответствии с ними нормативные акты подчинены Конституции и не могут ей противоречить.

Среди законов выделяют базовый для информационной сферы федеральный *ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»*, пришедший на смену ФЗ от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации».

Этими законами регулируются три группы взаимосвязанных между собой отношений, складывающихся:

– при осуществлении права на поиск, получение, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации (ЗИ).

К актам информационного законодательства федерального уровня относится *ФЗ от 29.11.1994 № 77-ФЗ «Об обязательном экземпляре документов»*. Данный нормативный акт определяет политику государства в области формирования обязательного экземпляра документов как ресурсной базы комплектования библиотечно-информационного фонда РФ и развития системы государственной библиографии, предусматривает обеспечение сохранности обязательного экземпляра документов, его общественное использование. Этим законом установлены виды обязательного экземпляра документов в категории их производителей и получателей, сроки и порядок доставки обязательного экземпляра документов, ответственность за их нарушение.

Видное место среди законов, регулирующих отношения в информационной среде, занимает *ФЗ РФ от 27.12.1991 № 2124 – 1 «О средствах массовой информации»*, представляющий собой комплексный нормативный акт, регламентирующий отношения, возникающие в процессе организации и функционирования средств массовой информации (СМИ). В основных разделах закона нашли правовое опосредование вопросы организации деятельности СМИ, распространения массовой информации, отношений СМИ с гражданами и организациями, прав и обязанностей журналиста, межгосударственного сотрудничества в области массовой информации, ответственности за нарушение законодательства о СМИ.

Особое место среди нормативных актов, регулирующих отношения по поводу информации, принадлежит *ФЗ РФ от 21.07.1993 № 5485 – 1 «О государственной тайне»*.

Один из законов, регулирующих отношения в информационной сфере, – *ФЗ РФ от 07.07.2003 № 126-ФЗ «О связи»*. Он устанавливает правовую основу деятельности в области связи, осуществляемой под юрисдикцией РФ, определяет полномочия органов государственной власти по регулированию этой деятельности, а также права и обязанности физических лиц, осуществляющих деятельность в области связи.

К законам, регулирующим информационные отношения, также относится и *ФЗ РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»*. Его цель – обеспечение правовых условий использование электронной подписи в электронных документах.

Отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников отношений, в том числе государства, на рынке товаров, работ и услуг, регулируются *ФЗ РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»*.

К нормативным актам данной проблематики относятся федеральные законы:

– от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»;

– от 12.05.2009 № 95-ФЗ «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами»;

– от 27.07.2006 № 152-ФЗ «О персональных данных»;

– от 28.12.2010 № 390-ФЗ «О безопасности»;

– от 28.07.2012 № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и др. законодательные акты.

Помимо названных выше существует множество законов, непосредственно не направленных на регулирование информационных отношений, но содержащих отдельные статьи, посвященные информации или связанные с ней. К числу следует отнести следующие федеральные законы:

– от 13.03.2006 № 38 -ФЗ «О рекламе»;

– от 29.12.1994 № 78-ФЗ «О библиотечном деле»;

– от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»;

– от 17.07.1999 № 176-ФЗ «О почтовой связи»;

– от 17.08.1995 № 147-ФЗ «О естественных монополиях»;

– от 21.02.1992 № 2395-1 «О недрах».

Часть норм, касающихся информационных отношений, содержатся в Гражданском кодексе РФ (ГК РФ). Так, ст. 150 относит личную и семейную тайну к нематериальным благам, ст. 726 устанавливает обязанность подрядчика передать информацию заказчику, ст. 857 посвящается банковской тайне, ст. 946 – тайне страхования. Четвертая часть ГК РФ направлена на регулирование отношений в области охраны прав на результаты интеллектуальной деятельности.

Среди подзаконных нормативных актов, регулирующих отношения в информационной сфере, можно выделить следующие:

а) указы Президента:

– от 11.02.2006 № 90 «О перечне сведений, отнесенных к государственной тайне»;

– от 06.10.2004 № 1286 «Вопросы межведомственной комиссии по защите государственной тайны»;

– от 17.05.2004 № 611 «О мерах по обеспечению безопасности РФ в сфере международного информационного обмена»;

– от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

– от 15.01.2913 № 31/с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

б) постановления Правительства:

– от 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства РФ и федеральных органов исполнительной власти»;

– от 27.05.2002 № 348 «Об утверждении Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;

– от 18.02.2005 № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий»;

– от 22.08.1908 № 1003 «О порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне»;

– от 28.10.1995 № 1050 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне»;

– от 26.10.2012 № 1101 «О создании единой автоматизированной системе «Единый реестр доменных имен, указателей страниц, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в РФ запрещено».

Наряду с указами Президента РФ и постановлениями Правительства источниками информационного права выступают акты центральных органов государственного управления РФ (ведомственные нормативно-правовые акты). В области информационных отношений существует значительное их количество. Тематика и направленность данных актов зависит от компетенции издавшего их органа.

Так, приказом Федеральной службы безопасности (ФСБ) РФ от 13.11.1999 № 564 утверждено «Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну», которое определяет организационную структуру системы сертификации, порядок проведения сертификации и инспекционного контроля, требования к нормативным и методическим документам по сертификации, а также виды средств защиты информации, подлежащих сертификации.

Приказом ФСБ РФ от 09.02.2005 № 66 утверждено «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации)».

Важный элемент системы законодательства РФ в информационной сфере – международные соглашения. В соответствии с ч. 4 ст. 15 Конституции РФ нормы международных договоров обладают приоритетом по отношению к противоречащим им правилам внутригосударственных законов. Это относится как к многосторонним, так и к двусторонним договорам.

Особое место среди многочисленных многосторонних соглашений, содержащих информационные нормы, занимают:

– «Всеобщая декларация прав человек» от 10.12.1948;

– «Международный пакт о гражданских и политических правах» от 10.12.1966;

– Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г.;

– «Заключительный акт совещания по безопасности и сотрудничеству в Европе» от 01.08.1975.

В этих документах нашли свое воплощение международные принципы и стандарты, провозглашающие право на свободу информации, которые, однако, налагают особые обязанности и особую ответственность, сопряженные с некоторыми ограничениями прав и свобод.

Важнейший документ, посвященный организации и активизации деятельности международного сообщества в области формирования глобального информационного общества, – «Окинавская хартия глобального информационного общества», принятая в июле 2000 г. представителями восьми ведущих стран. Этот документ устанавливает основные принципы вхождения государств в глобальное информационное общество.

**4.5. Перспективы развития законодательства в области информационной безопасности.**

|  |
| --- |
| Доктрина информационной безопасности Российской Федерации и конкретизирующие основные направления ее нормативного правового обеспечения, создают концептуальную основу для комплексного и взаимосвязанного развития законодательства в сфере обеспечения информационной безопасности. В современных условиях все страны должны разработать всеобъемлющие, перспективные и устойчивые национальные электронные стратегии. Ведущая роль в этом процессе должна принадлежать органам государственного управления. Частный сектор и гражданское общество, в диалоге с органами государственного управления, должны сыграть важную консультативную роль в формировании национальных электронных стратегий.  Укрепление доверия и безопасности при использовании информационных и коммуникационных технологий (ИКТ) является одним из ключевых принципов построения открытого информационного общества. При этом информационная безопасность и безопасность сетей (которые рассматриваются как два самостоятельных направления – razgovorodele.ru), вместе с защитой неприкосновенности частной жизни и прав потребителей составляют основу для доверия со стороны пользователей ИКТ.  Реализация указанного принципа предусматривает, в том числе:  а) укрепление доверия пользователей, повышение надежности и защиты целостности данных и сетей связи; анализа существующих и потенциальных угроз в области ИКТ и др.;  б) сотрудничество органов государственного управления с частным сектором в целях предупреждения и обнаружения актов киберпреступности и ненадлежащего использования ИКТ и реагирования на эти проявления;  в) просвещение пользователей относительно неприкосновенности частной жизни при работе в онлайновом режиме и способов ее защиты; г) принятие необходимых мер на национальном и международном уровнях для защиты от спама. Спам рассматривается как самостоятельная и серьезная проблема для пользователей сетей и в целом для Интернета;  д) проведение на национальном уровне оценки внутреннего законодательства с целью ликвидации препятствий для эффективного использования документов и осуществления сделок в электронной форме, в том числе использования электронных методов аутентификации;  е) обмен позитивным опытом в области информационной безопасности и безопасности сетей и поощрение его использования всеми заинтересованными сторонами;  ж) назначение координаторов для реагирования в режиме реального времени на происшествия в сфере безопасности и объединение этих координаторов в открытую сеть для обмена информацией и технологиями реагирования на происшествия.  В литературе справедливо обращается внимание на правовые аспекты защиты информации, которые могут возникнуть при недостаточно продуманном или злонамеренном использовании электронно-вычислительной техники. К ним относятся:  1. Регулирование юридической ответственности за искажение и подачу недостоверной информации.  2. Правовые вопросы защиты массивов информации от искажений и установления юридической ответственности по обеспечению сохранности информации.  3. Юридические и технические вопросы защиты хранящейся информации от несанкционированного доступа к ней, исключающие возможность неправомерного использования ее.  4. Установление юридически закрепленных норм и методов защиты авторских прав и приоритетов разработчиков программного продукта.  5. Разработка мероприятий по приданию юридической силы документам, выдаваемым машинами, и формирование юридических норм, определяющих лиц, ответственных за доброкачественность других документов.  6. Правовая защита интересов экспертов, передающих свои знания в фонды банков данных.  7. Установление правовых норм и юридической ответственности за использование электронно-вычислительных средств в личных интересах, противоречащих интересам других личностей и общества и могущих нанести им вред.  Сегодня совершенно понятна необходимость формирования, развития и внедрения глобальной культуры кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями. Это означает деятельность, направленную на предотвращение возможности использования ИКТ в целях, которые несовместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности, включая предотвращение использования информационных ресурсов и технологий в преступных и террористических целях.  Одним из элементов благоприятной среды для формирования и существования информационного общества названо верховенство права. Таким образом, определяется стратегия деятельности общества и государства в деле обеспечения информационной безопасности, включая перспективные задачи правового обеспечения этих процессов. Основные направления нормативного правового обеспечения информационной безопасности Российской Федерации конкретизируют эти задачи в среднесрочной перспективе.  Из числа первоочередных мер по совершенствованию нормативного правового обеспечения информационной безопасности, намеченных Основными направлениями нормативного правового обеспечения информационной безопасности Российской Федерации, в течение последних двух десятков лет приняты кодифицированные нормативные правовые акты, отдельные положения которых составляют нормативную базу информационной безопасности, в том числе: Гражданский процессуальный кодекс Российской Федерации, Арбитражный процессуальный кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Уголовно-процессуальный кодекс Российской Федерации, Гражданский кодекс Российской Федерации.  Анализ практики правового регулирования в сфере обеспечения информационной безопасности позволяет констатировать, что формирование правовой базы осуществляется недостаточно интенсивно, бессистемно, без должного анализа практики правоприменения и учета рекомендаций международных организаций, членом которых является Россия. Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям:  – не обеспечивается эффективная реализация и защита конституционных прав личности на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства (на это указывают масштабы неконтролируемого распространения баз, содержащих персональные данные, распространение таких данных в Интернете – razgovorodele.ru);  – не созданы благоприятные условия для свободного и оперативного доступа к информации органов государственной власти и органов местного самоуправления, непосредственно затрагивающей права и свободы личности, хотя начало положено формированием сайтов органов исполнительной власти;  – не обеспечена защита прав участников электронной коммерции, они работают на свой страх и риск, особенно велик этот риск у покупателей;  – отсутствуют правовые механизмы противодействия манипулированию информацией, что проявляется, с одной стороны, в невозможности легко проверить достоверность предоставляемой информации, а с другой стороны, в распространении средств и методов манипулирования информацией, особенно в рамках избирательных кампаний;  – увеличились масштабы нарушения прав интеллектуальной собственности, что связано с развитием Интернета, сложностью контроля за использованием в Сети объектов интеллектуальной собственности, распространением электронных библиотек, деятельность которых не регулируется;  – отсутствует защита интересов государства и общества в сфере использования государственных информационных ресурсов, не определены принципы отнесения информационных ресурсов к государственным и к национальному достоянию, не обеспечен беспрепятственный доступ к государственным ресурсам и порядок их создания, развития, поддержания.  Информационное общество не может быть построено по указанию свыше, это процесс, который требует деятельного участия бизнеса и гражданского общества. Наблюдаются позитивные изменения в позиции бизнеса по отношению к развитию законодательства. Для того чтобы этот диалог не прерывался, необходимо в разумных пределах сделать публичным процесс подготовки законопроектов в сфере информационной безопасности. |
| **Рекомендуемая литература:** |

1. Иваницкая Л.Н. Информационная безопасность. Хабаровск: ДВИУ-филиал РАНХиГС, 2016. – с. 60. – Режим доступа: – Режим доступа: <http://biblio.dvags.ru/MarcWeb/Pdf/NEWS/buk_trud9_infbez.pdf>.

2. Гафнер В.В. Информационная безопасность учебное пособие. Ростов на Дону: Феникс, 2010. – 324 с. – Режим доступа: http://xn 7sbabeyocb2bkdagddhcqh9acx1a8cxksc.xn--80afh5aqv.xn--p1ai/chitat-posobie/glava-1/1-1-ponyatie-informacii-i-informacionnoy-bezopasnosti/.

3. Баринов С.В. О правовом определении понятия информационная безопасность личности, 2016. – Режим доступа: <https://cyberleninka.ru/article/v/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti>.

**Контрольные вопросы:**

1. Дайте определения понятия «информационная безопасность», прокомментируйте его.

2. Что означает защита информации?

3. Назовите и раскройте содержание сфер ИБ.

4. Что является объектом ИБ?

5. Назовите виды угроз ИБ, раскройте их содержание.

5. Назовите группы источников угроз ИБ в соответствии с Доктриной информационной безопасности РФ.

6. Назовите факторы информационной безопасности личности.

7. В чем заключаются интересы личности в информационной сфере?

8. В чем заключаются интересы общества в информационной сфере?

9. В чем заключаются интересы государства в информационной сфере?

10. Чем является система обеспечения информационной безопасности РФ?

11. Назовите угрозы информационной безопасности Российской Федерации.

12. Назовите объекты правоотношений в области информационной безопасности.

13. Что собой представляет информационная система?

14. Что в себя включает средства обеспечения автоматизированных информационных систем и их технологий.

15. Что в себя включают основные технические средства?

16. Что в себя включают программные средства?

17. Что в себя включают лингвистические средства?

18. Назовите группы субъектов в области информационных технологий и средств их обеспечения.

19. Что собой представляет информационная инфраструктура?

20. Что собой представляет база данных (БД)?

21. Назовите угрозы информационной безопасности личности, охарактеризуйте их.

22. Назовите виды источников права в области ИБ.

23. Назовите уровни решения проблем ИБ, раскройте их содержание.

24. Назовите формы информационно-технических опасностей.

25. Назовите нормативные источники права в области ИБ.

26. Назовите законодательные акты в области ИБ, выделите сферу их применения.

27. Назовите подзаконные акты в области ИБ, выделите сферу их применения.

28. Назовите международные акты в области ИБ.

29. Назовите актуальные проблемы в области ИБ.

30. Назовите основные перспективы развития законодательства в области ИБ.