Тема 3. Правовые основы обеспечения информационной безопасности

1. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
2. Угрозы нарушения конфиденциальности, целостности, доступности информации.
3. Основные причины утечки информации.
4. Правовые средства обеспечения безопасности информации.

1. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках

Правовое обеспечение информационной безопасности представляет собой относительно самостоятельное направление информационного права, образуемое совокупностью правовых режимов, принципов и норм, закрепленных в законодательстве РФ и источниках международного права. В рамках данного направления информационного права регулируются общественные отношения по поводу обеспечения безопасности, прежде всего информации и информационной инфраструктуры, используемых человеком, обществом и государством для удовлетворения законных интересов, реализации прав и выполнения юридических обязанностей.

Правовой основой обеспечения информационной безопасности РФ являются:

- Доктрина информационной безопасности Российской Федерации
- Концепция Конвенции ООН об обеспечении международной информационной безопасности
- Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
- Основы государственной политики Российской Федерации в области международной информационной безопасности
- Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации
- Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

- Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

- Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

- Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

- Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

- Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

- Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

- Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

- Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

- Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

2. Угрозы нарушения конфиденциальности, целостности, доступности информации

Угроза нарушения конфиденциальности информации, способного нанести ущерб человеку, организации или государству в целом, его национальной безопасности заключается в создании условий для противоправного ознакомления с информацией ограниченного доступа лиц, не имеющих соответствующего разрешения обладателя информации, в том числе разрешения организации или уполномоченных федеральных органов исполнительной власти. К числу таких сведений могут относиться сведения о частной жизни, сведения, составляющие личную или семейную тайну, коммерческую или профессиональную тайну или государственную тайну.

Угрозы безопасности информации, связанные с нарушением законных интересов субъектов информационной сферы, могут также заключаться в нарушении целостности передаваемой информации, приводящем к невозможности ее использования в качестве средства реализации актов гражданского оборота или реализации актов органов публичной власти, местного самоуправления.

Угроза нарушения целостности передаваемой информации проявляется в возможности разрушения логических связей между элементами информационных баз данных, нарушения алгоритмов поиска, обобщения и представления заказчику недостоверной информации вследствие внедрения злоумышленниками на объектах

информационно-коммуникационной инфраструктуры продуктов, реализующих вредоносные информационные технологии.

Угроза недоступности законной информации проявляется в неправомерном блокировании доступа к общедоступной информации и информации, относящейся к национальному достоянию, и, соответственно, — в ущемлении конституционных прав человека и гражданина в поиске и получении информации.

3. Основные причины утечки информации

Утечка информации – это несанкционированный доступ к закрытым данным и неконтролируемое распространение секретных сведений в результате их разглашения.

Главные причины утечки информации:

- нарушение сотрудниками требований в работе с источниками служебной информации и правил использования систем защиты;
- недочёты в конструировании систем защиты;
- проведение злоумышленником технической и агентурной разведок.

Виды утечки информации:

- разглашение;
- несанкционированный доступ к информации;
- получение секретной информацией разведками.

Под разглашением информации понимается запрещённая передача служебной или секретной информации до людей, не имеющих на неё права.

Под несанкционированным доступом понимается получение запрещённой информации ложным или обманным путём лицом, не имеющим на неё права.

Получение секретной информации разведками может осуществляться с помощью технических средств или агентурными методами.

4. Правовые средства обеспечения безопасности информации

Общая структура правовых средств обеспечения безопасности информации включает:

Правовые средства противодействия угрозе недоступности информации включают прежде всего:

— запрет на ограничение доступа к определенным видам информации: к общедоступной информации, к которой относятся общеизвестные сведения и иная информация, доступ к которой не ограничен; к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления; к информации о состоянии окружающей

среды; к информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайны); к информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией; к иной информации, недопустимость ограничения доступа к которой установлена федеральными законами;

— дозволения обладателям информации, другим лицам, обладающим информацией па законном основании, предоставлять возможность свободно использовать информацию любому лицу и передавать одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения, а также обжаловать в вышестоящий орган или вышестоящему должностному лицу либо в суд решения на действие (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающих право на доступ к информации.

Правовые средства противодействия угрозе недостоверности информации в отношении отражаемых объектов и явлении окружающей действительности включают:

— позитивную обязанность владельца сайта и (или) страницы сайта в сети Интернет, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети Интернет (далее — блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данных сайте или странице сайта иными пользователями сети Интернет, обеспечивать соблюдение законодательства Российской Федерации, в частности проверять достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;

— запрет при размещении информации на сайте или странице сайта в сети Интернет, использовании сайта или страницы сайта в сети Интернет в целях сокрытия или фальсификации общественно значимых сведений, распространении заведомо недостоверной информации под видом достоверных сообщений.

Правовые средства противодействия угрозе использования информации для разжигания национальной, социальной розни, пропаганды и агитации, возбуждающих национальную рознь, пропаганды сепаратизма, терроризма и экстремизма включают:

— запрет на распространение в Российской Федерации информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

— запрет владельцу сайта и (или) страницы сайта в сети Интернет, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети Интернет, допускать использование сайта или страницы сайта в сети Интернет в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

— позитивная обязанность блогера размещать на своих сайте или странице сайта в сети Интернет свои фамилию и инициалы, электронный адрес для направления ему юридически значимых сообщений, а также опубликовывать на данных сайте или странице

сайта незамедлительно при получении решение суда, вступившего в законную силу, содержащееся в решении требование.

Правовые средства противодействия угрозе нарушения конфиденциальности информации, способного нанести ущерб человеку, организации или государству включают:

— позитивную обязанность по отнесению в соответствии с требованиями законодательства информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, по соблюдению конфиденциальности такой информации, по ответственности за ее разглашение, а также по защите информации, полученной гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональной тайны), в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации;

— позитивную обязанность предоставлять третьим лицам информацию, составляющую профессиональную тайну в соответствии с федеральными законами и (или) по решению суда;

— позитивная обязанность прекратить по требованию уполномоченного органа размещение информации в форме открытых данных, если это может привести к распространению сведений, составляющих государственную тайну;

— запрет ограничения срока исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, без согласия гражданина (физического лица), предоставившего такую информацию о себе, а также запрет требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами;

— запрет на использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов.

Правовые средства противодействия угрозе неправомерного использования результатов интеллектуальной деятельности включают:

— дозволение рассматривать и разрешать споры, связанные с защитой нарушенных или оспоренных интеллектуальных прав, судом;

— дозволение правообладателям, а также организациям по управлению правами на коллективной основе, иных лиц, в случаях установленных законом, использовать для защиты интеллектуальных прав способы, предусмотренные законодательством;

— дозволение правообладателям при защите исключительных прав предъявлять требования о признании права, о пресечении действий, нарушающих право или создающих угрозу его нарушения, о возмещении убытков, об изъятии материального носителя, об опубликовании решения суда о допущенном нарушении.

Правовые средства противодействия угрозе нарушения целостности передаваемой информации включают:

— позитивную обязанность операторов информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, создавать и эксплуатировать такие системы в соответствии с требованиями, установленными законодательством;

— запрет эксплуатации государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности;

— позитивную обязанность операторов государственных информационных систем обеспечить соответствие программно-технических средств и средств защиты информации требованиям законодательства РФ о техническом регулировании, а также достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы;

— позитивную обязанность обладателя информации, оператора информационной системы в случаях, установленных законодательством РФ, обеспечить:

— предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

— своевременное обнаружение фактов несанкционированного доступа к информации; предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

— недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

— возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

— постоянный контроль за обеспечением уровня защищенности информации;

— нахождение на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.