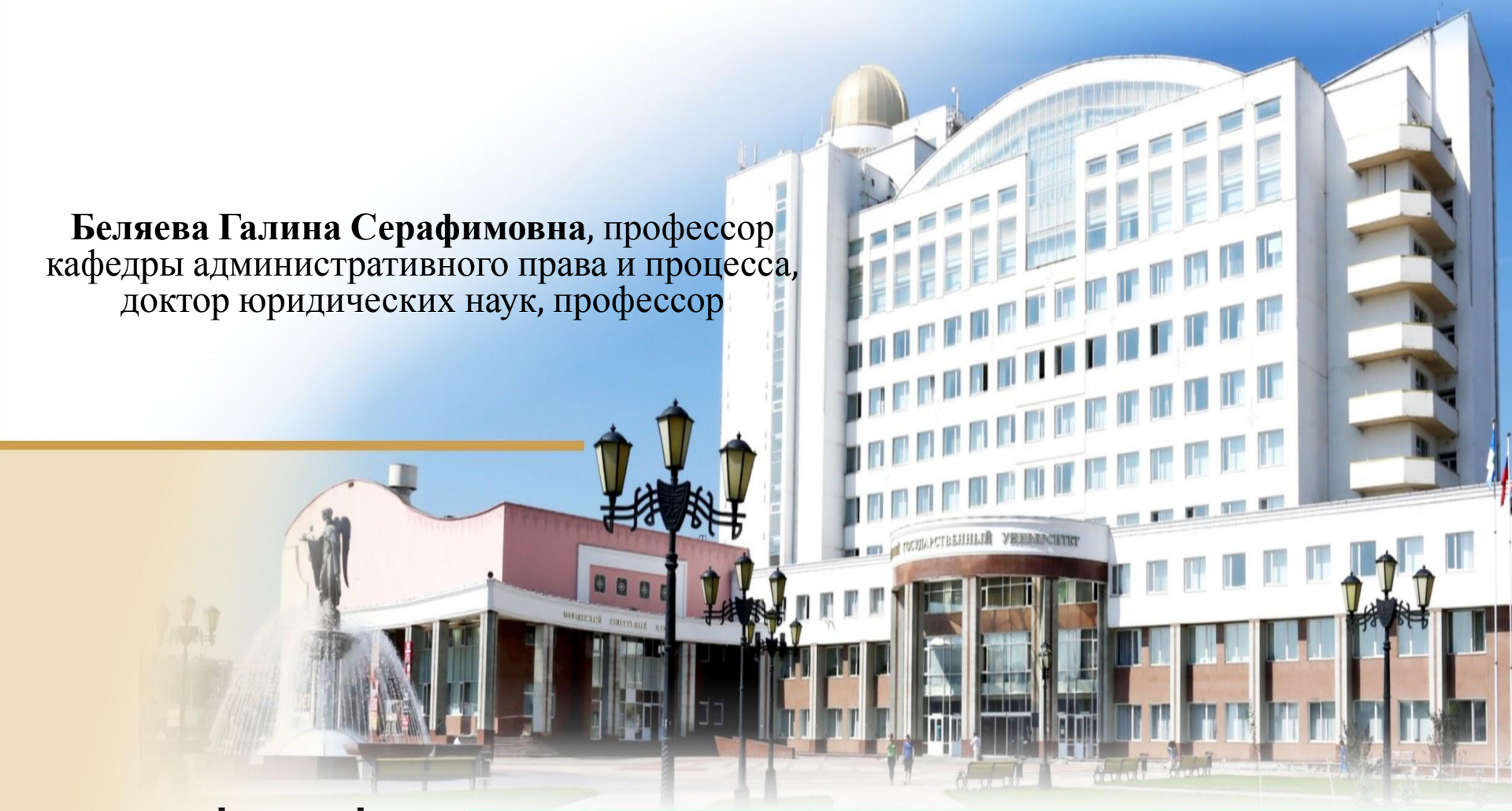
Темы 6. Информационная безопасность

НИУ БелГУ
BELGOROD STATE UNIVERSITY (BelSU)

Беляева Галина Серафимовна, профессор кафедры административного права и процесса, доктор юридических наук, профессор



План лекции:

1. Общие положения Доктрины информационной безопасности Российской Федерации.
2. Национальные интересы в информационной сфере.
3. Основные информационные угрозы и состояние информационной безопасности.
4. Стратегические цели и основные направления обеспечения информационной безопасности.
5. Организационные основы обеспечения информационной безопасности.

Источники:

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Доктрина является

- **документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации,** в котором развиваются положения **Стратегии национальной безопасности Российской Федерации,** утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере;
- **основой** для формирования **государственной политики** и **развития общественных отношений в области обеспечения информационной безопасности,** а также для выработки мер по совершенствованию **системы обеспечения информационной безопасности.**

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере

Информационная сфера – совокупность

- информации,
- объектов информатизации,
- информационных систем,
- сайтов в информационно-телекоммуникационной сети "Интернет",
- сетей связи,
- информационных технологий,
- субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности,
- а также совокупность механизмов регулирования соответствующих общественных отношений.

Термины и определения

а) **национальные интересы Российской Федерации в информационной сфере** – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) **угроза информационной безопасности Российской Федерации** – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) **информационная безопасность Российской Федерации** – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) **обеспечение информационной безопасности** – осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) **силы обеспечения информационной безопасности** – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

е) **средства обеспечения информационной безопасности** – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

ж) **система обеспечения информационной безопасности** – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

з) **информационная инфраструктура Российской Федерации** – совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

В Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены **стратегические цели** и **основные направления** обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Национальные интересы в информационной сфере

а) **обеспечение и защита конституционных прав и свобод человека и гражданина** в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) **обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры**, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) **развитие в Российской Федерации отрасли информационных технологий и электронной промышленности**, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) **доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации** и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) **содействие формированию системы международной информационной безопасности**, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной

Реализация национальных интересов в информационной сфере **направлена** на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Основные информационные угрозы и состояние информационной безопасности

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.

Практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Основные информационные угрозы и состояние информационной безопасности (продолжение)

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.

Основные информационные угрозы и состояние информационной безопасности (окончание)

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

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,

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**

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

Стратегическая цель обеспечения информационной безопасности Российской Федерации в области обороны страны

защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

Стратегическая цель обеспечения информационной безопасности в области государственной и общественной безопасности

защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры

Основные направления

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

Основные направления обеспечения информационной безопасности в области государственной и общественной безопасности (продолжение)

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных

Стратегическая цель обеспечения информационной безопасности в экономической сфере

сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности

Основные направления

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, В структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги В области обеспечения информационной безопасности, В том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на

Стратегическая цель обеспечения информационной безопасности в области науки, технологий и образования

поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности

Основные направления обеспечения информационной безопасности в области науки, технологий и образования

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Стратегическая цель обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства

формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве

Основные направления обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства

а) защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов В информационной сфере;

б) участие в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

в) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

г) продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

д) развитие национальной системы управления российским сегментом сети "Интернет"

Организационные основы обеспечения информационной безопасности

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

СОСТАВ
системы обеспечения информационной безопасности

определяется Президентом Российской Федерации

Организационная основа системы обеспечения информационной безопасности

- Совет Федерации Федерального Собрания Российской Федерации,
- Государственная Дума Федерального Собрания Российской Федерации,
- Правительство Российской Федерации,
- Совет Безопасности Российской Федерации,
- федеральные органы исполнительной власти,
- Центральный банк Российской Федерации,
- Военно-промышленная комиссия Российской Федерации,
- межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации,
- органы исполнительной власти субъектов Российской Федерации,
- органы местного самоуправления,
- органы судебной власти, принимающие в соответствии с

УЧАСТНИКИ
системы обеспечения информационной безопасности

- собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты,
- средства массовой информации и массовых коммуникаций,
- организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка,
- операторы связи,
- операторы информационных систем,
- организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности,
- организации, осуществляющие образовательную деятельность в данной области,
- общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

ПРИНЦИПЫ ДЕЯТЕЛЬНОСТИ
государственных органов по обеспечению информационной безопасности

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

ЗАДАЧИ
государственных органов в рамках деятельности по обеспечению информационной безопасности

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

НИУ БелГУ
BELGOROD STATE UNIVERSITY (BelSU)

СПАСИБО ЗА ВНИМАНИЕ!