Политика Российской Федерации в области кибербезопасности
Policy of the Russian Federation in the field of cybersecurity

С.И. Луценко[1]

Эксперт НИИ Корпоративного и проектного управления (г. Москва). Аналитик Института экономический стратегий Отделения общественных наук Российской академии наук.

Соавтор документа «Стратегия развития электросетевого комплекса Российской Федерации».
Автор проекта «Контуры Концепции развития финансового кластера Российской Федерации на долгосрочную перспективу»
E-mail: scorp_ante@rambler.ru

S.I. Lutsenko

Lutsenko Sergej Ivanovich, Expert, The Corporate and Project Management Institute (Moscow), Analyst, Institute for Economic Strategies of the Social Sciences Division of the Russian Academy of Sciences (Moscow).
The co-author of the document «Strategy of development of an electric grid complex of the Russian Federation».
The author of the project «Contours of the Concept of Developing Financial Cluster of the Russian Federation in the Long-Term Period».

Автор рассматривает особенности информационной безопасности с учетом возможных потенциальных угроз, в том числе внешних. Действующая Доктрина информационной безопасности Российской Федерации требует серьезной корректировки, в части вопросов кибербезопасности.

The author considers features of information security taking into account possible potential threats, including external. The Doctrine of information security of the Russian Federation demands serious adjustment, regarding cybersecurity questions.

Ключевые слова: кибербезопасность, доктрина национальной безопасности, угроза, информационные технологии, информационная безопасность

Keywords: cybersecurity, the doctrine of national safety, threat, information technology, information security

В Доктрине информационной безопасности России [7], под информационной безопасностью понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. Правовыми методами называются: разработка и неуклонная реализация требований нормативных правовых актов, регламентирующих отношения в информационной сфере и нормативно-методических документов по вопросам обеспечения информационной безопасности РФ. Приоритетным направлением государственной политики в сфере обеспечения информационной безопасности в РФ является совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере.

[1] Автор благодарит за идею статьи и сюжетную линию Чеснокова А.Н.

В доктрине не определены наиболее распространенные угрозы информационной безопасности. В частности, определение кибербезопасности, и ее производные составляющие.

В настоящее время, трансформация систем глобального управления и переход к многополярности, усиление борьбы за сферы влияния, рост региональной нестабильности, привели к обострению мировых проблем безопасности, в том числе кибербезопасности.

Информационные технологии приобрели глобальный трансграничный характер. Это способствует развитию всех сфер деятельности человека, общества и государства. Эффективное применение информационных технологий становится фактором, который позволяет ускорить экономическое развитие страны и совершенствовать функционирование различных институтов.

Основными источниками угроз в сфере информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных групп и формирований, противозаконная деятельность отдельных лиц, нарушение установленных регламентов сбора, обработки и передачи информации, преднамеренные действия и непреднамеренные ошибки персонала информационных систем, отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

Источники угроз информационной безопасности разделяются на угрозы, источник которых расположен вне контролируемой зоны (внешние), и угрозы, источник которых расположен в пределах контролируемой зоны (внутренние).

К внешним угрозам информационной безопасности относятся: деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных систем; перехват и утечка информации по техническим каналам; неконтролируемое самопроизвольное распространение компьютерных вирусов и иных вредоносных программ; стихийные бедствия, катастрофы, пожары и аварии.

Внутренними угрозами информационной безопасности являются: невыполнение требований действующего законодательства и несвоевременное принятие необходимых правовых актов, регламентирующих деятельность в сфере информационной безопасности; нарушения установленных регламентов сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, создающие предпосылки к утечке либо разглашению сведений, составляющих государственную, служебную и иную тайну; внедрение несовершенных или устаревших информационных технологий и средств информатизации; умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала; отказы, сбои, неисправности, несогласованности инженерно-технических, программных и системно-прикладных средств защиты информационных и телекоммуникационных систем; использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты и контроля информации в случаях, когда такое требование законодательно установлено; привлечение к работам по созданию, развитию и защите информационных систем организаций, не имеющих лицензии на данный вид деятельности.

Непрерывный процесс прогнозирования, выявления, идентификации, конкретизации, анализа и выработки мер по локализации угроз является неотъемлемой задачей деятельности по построению системы информационной безопасности.

Возрастает количество информационных систем, функционирующих во многих сферах: здравоохранении, образовании, жилищно-коммунальном хозяйстве, банковском секторе, энергетике, торговле, на транспорте и в коммуникациях.

Одновременно с развитием технологий все большее значение приобретает защита от пропорционально растущего числа киберугроз. Значит, все более актуальными и осново-

полагающими становятся вопросы, связанные с обеспечением информационной безопасности.

Активное использование облачных технологий, внедрение Big Date, распространение интернета вещей (IoT) представляют собой фундаментальные факторы, влияющие на кибербезопасность.

Объем данных, обрабатываемых в государственном и частном секторах, растет, что приводит к необходимости выработки новых форм их хранения. В тоже время, такие формы хранения данных как облачное хранилище или использование онлайн - сервисов часто основываются операторами и поставщиками услуг на непрозрачных или не стандартизованных решениях, в том числе с точки зрения безопасности данных. При этом гармонизированные стандарты значительно отличаются от первоисточника из-за низкого качества их перевода и адаптации.

Ситуация усугубляется возможностью намеренного внедрения в программное обеспечение и телекоммуникационное оборудование не декларируемых функций (так называемых «бэкдоров»), которые не всегда могут быть выявлены на этапе сертификации, устранения уязвимостей в процессе эксплуатации или распознаны антивирусными программами и потому могут быть использованы для нарушения работы информационных систем и сетей телекоммуникаций.

Транснациональный и трансграничный характер многих продуктов информационно - коммуникационных технологий (далее - ИКТ) и международная связанность сетей телекоммуникаций общего пользования используются преступностью в целях совершения противоправных действий в отношении пользователей и операторов ИКТ-услуг и владельцев Интернет-ресурсов, размещенных в национальном сегменте, а также информационных систем, взаимодействующих с Интернетом.

Российская Федерация в сфере кибербезопасности испытывает такие серьезные угрозы как: низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности; нарушение государственными и негосударственными субъектами информатизации и пользователями услуг в сфере ИКТ установленных требований, технических стандартов и регламентов сбора, обработки, хранения и передачи информации в электронной форме; непреднамеренные ошибки персонала и технологические сбои, оказывающие негативное воздействие на информационные системы, программное обеспечение и другие элементы информационно - коммуникационной инфраструктуры; действия международных преступных групп, сообществ и отдельных лиц по осуществлению хищений в финансово - банковской сфере, вредоносного воздействия в целях нарушения работы автоматизированных систем управления технологическими процессами промышленности, энергетики, связи и в сфере информационно - коммуникационных услуг; деятельность политических, экономических, террористических структур, разведывательных и специальных служб иностранных государств, направленная против интересов Российской Федерации, путем оказания разведывательного и подрывного воздействия на информационно - коммуникационную инфраструктуру.

Необходимо отметить, что понятие «кибербезопасность» и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого общепризнанного юридического определения на международном уровне.

Тем не менее, кибербезопасность - это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз

безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и неотказуемость; конфиденциальность [1].

На уровне ООН имеется ряд документов, таких как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур", в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования информационно - коммуникационных технологий в вопросах обеспечения (1) неприкосновенности частной жизни, (2) конфиденциальности, целостности и доступности информации в электронной форме, (3) защиты критической информационно - коммуникационной инфраструктуры, взаимодействующей с Интернетом (в том числе информационных систем, аппаратно - программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации, программного обеспечения) от вредоносного воздействия программно - техническими методами.

Отдельные страны рассматривают через призму кибербезопасности только неконтролируемое распространение в Интернете, как всемирной системе объединенных сетей телекоммуникаций и вычислительных ресурсов, электронных материалов, пропагандирующих терроризм, детскую порнографию и некоторые виды незаконной информации, в первую очередь, по причине технической сложности установления источника распространения такой информации.

Как следствие, различаются и подходы к составлению стратегий кибербезопасности. Тем не менее, руководящие документы, охватывающие вопросы кибербезопасности, как правило, предусматривают: построение государственной системы управления в сфере обеспечения кибербезопасности; определение соответствующего механизма (в основном общественно - государственного партнерства), позволяющего частным и государственным заинтересованным сторонам обсуждать проблемы обеспечения безопасности национальных информационных инфраструктур; определение необходимой политики безопасности и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально - технического обеспечения).

Как свидетельствует мировой опыт, полную защиту от ошибок в программном обеспечении или инцидентов информационной безопасности достигнуть невозможно, но путем осознанного ответственного поведения снизить их частоту и вероятность, обеспечить высокую скорость восстановления работоспособности информационных систем и ресурсов, чтобы не допустить разрушительных последствий, жизненно необходимо.

Государство прилагает много усилий, чтобы защитить наше кибернетическое пространство и информационные системы. Для этого создает взаимоувязанную систему правовых, технических и организационных мер. Их задача - противодействовать угрозам информационной безопасности.

В то же время в правовых режимах различных типов информации есть существенные отличия. Это требует более детальной классификации систем, в которых обрабатывается информация. Только при таком подходе можно принимать эффективные и достаточные меры технической защиты информации.

В связи с указанным необходимо совершенствовать механизмы правового регулирования деятельности в области защиты информации.

Интересным представляется опыт Республики Казахстан, в отношении выработки основных направлений в борьбе против потенциальных угроз в контексте информационной безопасности [3].

Формирование необходимых условий для повышения осведомленности об угрозах, развития человеческого капитала и потенциала отечественной отрасли ИКТ по созданию

программных продуктов и систем кибербезопасности, направленных на блокирование и подавление вредоносного программно - технического воздействия и защищенного телекоммуникационного оборудования.

Совершенствование правоприменительной практики, методологической базы, нормативно - правового и организационно - технического обеспечения безопасного использования ИКТ в национальной системе защиты информации и безопасности автоматизированных систем управления технологическими процессами.

Наконец, создание высоко адаптивной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно - коммуникационной инфраструктуры.

Предоставление приоритета исследованиям и собственной школе прикладной математики, по разработке средств криптографической защиты информации, криптологии, разработок по программируемым логическим интегральным схемам, квантовой криптографии и разработке защиты систем передачи, обработки и хранения информации, а также систем информационной безопасности.

Преодоление проблемы не высокой востребованности отечественных разработок, т.к. кибербезопасность в конечном итоге зависит от уровня развития отечественной IT-отрасли и электронной промышленности. Одной из причин этого является отсутствие обязательности приоритетного использования их продукции в государственных органах.

Установление мер по их поддержке, в том числе через стимулирование государственно - частного партнерства повышения конкурентоспособности. Критериями должны стать соответствие требованиям локализации разработки и технической поддержки, наличие у поставщика исключительных прав интеллектуальной собственности на конструкторскую и техническую документацию программных продуктов и телекоммуникационного оборудования, а также наличие научно - производственной базы, необходимой для организации производства, гарантийного и послегарантийного обслуживания.

Для полноценной оценки состояния защищенности объектов информатизации с учетом характера деятельности киберпреступников и иностранных технических компьютерных разведок, рассчитывающих на самоуспокоенность и небрежность со стороны владельцев информационных ресурсов и систем, необходимо стремиться к непрерывному мониторингу состояния информационных систем и ресурсов техническими средствами контроля защищенности и проведению работы по выявлению каналов утечки информации (уязвимостей, вирусов, троянских программ, недекларируемых функций и закладок).

Такой подход позволит обеспечить сохранение возможности реализации государственных функций в случае чрезвычайных происшествий технологического, социального характера, вызванных инцидентами информационной безопасности, угрожающими национальной и общественной безопасности, а в случае чрезвычайного или военного положения возможности использования устойчивой информационно - коммуникационной инфраструктуры сил обеспечения национальной безопасности в интересах функционирования критически важных объектов информационно - коммуникационной инфраструктуры.

Для создания высоко адаптированной и интегрированной системы государственного управления информационной безопасностью в сфере информатизации и связи в отношении всей национальной информационно - коммуникационной инфраструктуры предлагается: государственным органам и поставщикам услуг принять риск- ориентированный подход к безопасности, уделяя первоочередное внимание усилиям, которые обеспечивают наиболее высокий уровень надежности создаваемых информационных систем в нормальном и внештатном режимах и устойчивости их к умышленным сбоям.

Расширить взаимодействие между ведомственными и отраслевыми структурами мониторинга и реагирования на инциденты информационной безопасности для оказания содействия владельцам информационных ресурсов и систем и взаимного оповещения о возникающих угрозах. Их участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования, проектирования, разработки и эксплуатации

отраслевых информационных систем и сетей и стать опорными точками, определяющими устойчивость всей информационно - коммуникационной инфраструктуры страны.

Опыт Республики Казахстан в части отдельных элементов информационной безопасности можно было бы перенести в российскую правовую плоскость.

Интересным представляется опыт Республики Беларусь в отношении кибербезопасности.

В частности, в соответствии с главами 16 и 17 Постановления Совета Безопасности Республики Беларусь «О Концепции информационной безопасности Республики Беларусь» [4], в качестве наиболее вероятных источников угроз кибербезопасности рассматриваются отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах, противоправная деятельность отдельных лиц и преступных групп, преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации, зависимость Беларуси от других стран - производителей программных и аппаратных средств при создании и развитии информационной инфраструктуры.

Национальная система обеспечения кибербезопасности должна реализовывать весь возможный комплекс правовых, организационных и технических мер по обеспечению безопасности национальной информационной инфраструктуры, в том числе информационных систем, обеспечивать конфиденциальность, доступность и целостность информации, а также легко трансформироваться и адаптироваться в изменяющейся обстановке за счет постоянного анализа на предмет соответствия актуальным рискам кибербезопасности.

Приоритетной задачей в контексте кибербезопасности рассматривается создание единой государственной системы мониторинга национального сегмента сети Интернет с одновременным формированием облачной платформы предоставления комплексных сервисов информационной безопасности государственному сектору и бизнес-сообществу в интересах автоматизированного учета киберинцидентов и оперативного обмена информацией о них между уполномоченными государственными органами, операторами электросвязи и командами быстрого реагирования на компьютерные инциденты (CERT/CSIRT). В перспективе также рассматривается формирование экосистемы для создания и функционирования национального удостоверяющего центра, корневой сертификат которого будет являться доверенным для основных операционных систем и веб-браузеров.

Более того, Конституционный Суд Республики Беларусь в своем решении от 14.03.2019 № Р-1166/2019 отмечает, что усиление роли информатизации и цифровизации на современном этапе, правовое регулирование общественных отношений в информационной сфере должно являться приоритетным. В этих целях необходимо принятие нормативных правовых актов, направленных на защиту персональных данных граждан, обеспечение информационного суверенитета и кибербезопасности страны.

Логическим продолжением работы в сфере информационной безопасности в Республике Беларусь стало принятие новой редакции приказа Оперативно-аналитического центра при Президенте «О некоторых вопросах технической и криптографической защиты информации» [5].

В частности, в приказе уточняются требования к анализу уязвимостей в информационных системах при проведении аттестации, что, в свою очередь, потребует от лицензиата приобрести специализированные технические средства.

Информацию, ограниченную для распространения и (или) предоставления, но не отнесенную к государственным секретам, следует обрабатывать с применением системы защиты, аттестованной Оперативно-аналитическим центром при Президенте.

В Российской Федерации на уровне регионов принимаются нормативные акты, регулирующие направления информационной безопасности.

В частности, в соответствии с Распоряжением Правительства Иркутской области «О Концепции развития и эффективного использования информационных систем исполни-

тельных органов государственной власти Иркутской области и информационного общества в Иркутской области до 2020 года» [6] определены направления обеспечения информационной безопасности, принципы, а также методы, способы и средства защиты информации, необходимые для обеспечения безопасности информации.

Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

Основные направлениями обеспечения информационной безопасности являются: правовое обеспечение информационной безопасности (деятельность, направленная на создание и поддержание в актуальном состоянии системы локальных нормативных актов, регламентирующих деятельность по обеспечению информационной безопасности); организация работы по обеспечению информационной безопасности (деятельность, направленная на создание документированных процессов обеспечения информационной безопасности, скоординированных между исполнительными органами государственной власти Иркутской области); обеспечение информационной безопасности при управлении информационными ресурсами (деятельность, направленная на идентификацию, классификацию информационных ресурсов и их владельцев, формирование и поддержание необходимого уровня информационной безопасности информационных ресурсов); обеспечение информационной безопасности, связанное с персоналом (деятельность, направленная на минимизацию рисков, вызванных действиями работников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки уровня знаний всех работников по вопросам обеспечения информационной безопасности); физическая безопасность информационных ресурсов (деятельность, направленная на минимизацию и предотвращение ущерба, вызванного физическим воздействием на информационные ресурсы); обеспечение информационной безопасности на этапах жизненного цикла информации в информационной инфраструктуре (деятельность, направленная на минимизацию рисков, возникающих в процессе создания, обработки, обмена и уничтожения информации в информационной инфраструктуре); управление доступом к информационным ресурсам (деятельность, направленная на создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа); управление инцидентами информационной безопасности (деятельность, направленная на создание процесса или процессов по своевременному выявлению и реагированию на инциденты информационной безопасности).

Реализация основных направлений информационной безопасности осуществляется на основе следующих принципов: принцип законности - осуществление защитных мероприятий и разработки системы информационной безопасности в соответствии с действующим законодательством в области информационных технологий и защиты информации; принцип персональной ответственности - ответственность в пределах должностных обязанностей за несоблюдение регламентирующих документов в области информационной безопасности; принцип минимизации полномочий - предоставление прав доступа сотрудникам исполнительных органов государственной власти Иркутской области к информационным ресурсам в объеме, достаточном для качественного выполнения своих должностных обязанностей; принцип своевременности - своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружения угроз, потенциально способных нанести ущерб; принцип системности - подход к построению системы информационной безопасности с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблем обеспечения информационной безопасности, включающего фазы планирования, реализации, контроля и ее совершенствования; принцип комплексного подхода - всестороннее обеспечение информационной безопасности, то есть использования программно-технических, организационных, правовых, нормативно-методических и других мер обеспечения информационной безопасности на единой кон-

цептуальной основе; принцип непрерывности - постоянный целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных мер защиты. Должно предусматриваться комплексное использование методов и средств защиты: согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному нарушителю требовались профессиональные навыки в нескольких невзаимосвязанных областях. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей должны быть средства криптографической защиты, используемые для создания виртуальных частных сетей. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты; принцип унифицированности - унификация принципов, правил, процедур, требований и технических решений по обеспечению информационной безопасности; принцип простоты - понятность пользователю порядка действий и процесса использования средств обеспечения информационной безопасности и защиты информации.

При выборе и использовании комплекса методов, способов и средств защиты информации, необходимых для обеспечения безопасности информации в конкретных информационных системах, учитываются: наличие конфиденциальной информации (персональные данные, служебная тайна и т.д.); условия размещения и эксплуатации технических средств; способы обработки данных в информационной системе; особенности обработки и пересылки информации в электронном виде; количество пользователей и способы организации их работы с информационной системой; способы хранения информации.

Проблема обеспечения информационной безопасности может быть решена в результате комплексного применения всех мер защиты, включающих в себя: правовые меры обеспечения информационной безопасности; организационные меры обеспечения информационной безопасности; технические меры обеспечения информационной безопасности.

Применение технических мер обеспечения информационной безопасности должно осуществляться с использованием технических и программных комплексов, сертифицированных по требованиям безопасности информации Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

Проведение аттестации объектов информатизации на соответствие требованиям безопасности информации также осуществляется в соответствии с законодательством Российской Федерации.

Необходимо отметить, что технические меры обеспечения информационной безопасности основываются на использовании программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

Технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать: идентификацию и аутентификацию субъектов доступа и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защиту машинных носителей информации; регистрацию событий безопасности; антивирусную защиту; обнаружение (предотвращение) вторжений; контроль (анализ) защищенности информации; целостность информационной системы и информации; доступность информации; защиту среды вирту-

ализации; защиту технических средств; защиту информационной системы, ее средств, систем связи и передачи данных.

Контроль состояния информационной безопасности осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации, а также соблюдения установленных правил эксплуатации систем защиты информации. Основная задача контроля - получение объективных оценок текущего состояния защиты информации ограниченного распространения, оценка эффективности применяемых мер и технических решений для обеспечения информационной безопасности, оказание методической помощи по обеспечению режима защиты информации, организация работы по обеспечению информационной безопасности.

Причем, каждый исполнительный орган государственной власти Иркутской области осуществляет внутренний контроль состояния информационной безопасности его информационных систем. В указанных целях для получения дополнительного заключения об их состоянии привлекаются к выполнению контроля и аудита администраторы безопасности информации других исполнительных органов государственной власти Иркутской области, а также специалисты организаций, обладающих соответствующими правами на осуществление деятельности в области защиты информации.

Общий контроль, координацию деятельности и разработку методических рекомендаций по технической защите информации в отношении исполнительных органов государственной власти Иркутской области осуществляет аппарат Губернатора Иркутской области и Правительство Иркутской области.

Аппарат Губернатора Иркутской области и Правительство Иркутской области осуществляет выборочные проверки состояния технической защиты информации в исполнительных органах государственной власти Иркутской области.

Оценка эффективности мер информационной безопасности проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Аналогичный нормативный акт принят и на территории Нижегородской области [2].

В качестве, основных принципов развития системы информационной безопасности Нижегородской области определены: соответствие уровня развития системы информационной безопасности Нижегородской области задачам обеспечения национальной безопасности Российской Федерации, безопасности и устойчивого развития Нижегородской области с учетом ее ресурсных возможностей; соответствие системы информационной безопасности Нижегородской области требованиям действующего законодательства; обеспечение на территории Нижегородской области своевременной и адекватной реакции на возникающие и прогнозируемые угрозы безопасности информации; использование коллегиальных методов руководства системой информационной безопасности Нижегородской области и ее развития; наконец, программно-целевое планирование развития системы ИБ Нижегородской области.

Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов: конфиденциальность, целостность и доступность. Характерная для последних десятилетий общемировая тенденция внедрения достижений информационно - коммуникационных технологий с темпами, существенно опережающими формирование культуры их использования, и укоренения общественных и производственных отношений, характерных для «информационного общества», в первую очередь, в вопросах обеспечения кибербезопасности. На сегодняшний день, российской доктрине информационной безопасности требуется корректировка, в части, вопросов кибербезопасности: построение государственной системы управления в сфере обеспечения кибербезопасности; определение соответствующего механизма (государственно-частного партнерства), позволяющего частным и государственным заинтере-

сованным сторонам обсуждать проблемы обеспечения безопасности национальных информационных инфраструктур; формулирование политики безопасности и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для акторов.

Литература

1. Постановление Правительства Воронежской обл. от 26.03.2014 № 245 «Об утверждении прогноза научно-технологического развития Воронежской области до 2030 года» // Доступ из СПС «Консультант Плюс».
2. Постановление Правительства Нижегородской области от 31.12.2015 № 920 «Об утверждении Концепции информационной безопасности Нижегородской области» // Доступ из СПС «Консультант Плюс».
3. Постановление Правительства от 30.06.2017 № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан») // Доступ из СПС «Консультант Плюс».
4. Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь» // Доступ из СПС «Консультант Плюс».
5. Приказ Оперативно-аналитического центра при Президенте от 30.08.2013 № 62 «О некоторых вопросах технической и криптографической защиты информации» // Доступ из СПС «Консультант Плюс».
6. Распоряжение Правительства Иркутской области от 08.02.2016 № 44-рп «О Концепции развития и эффективного использования информационных систем исполнительных органов государственной власти Иркутской области и информационного общества в Иркутской области до 2020 года» // Доступ из СПС «Консультант Плюс».
7. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50.