**МВД России**
**Санкт-Петербургский университет**

# ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

**Учебное пособие**

**Санкт-Петербург**
**2023**

План-график 2023, поз. 42

**УДК 004.7**
**ББК 32.88**
**О 64**

**О 64** **Организационно-правовые основы технической защиты конфиденциальной информации:** учебное пособие / под общ. ред. Ю.И. Синещука. – Санкт-Петербург: СПбУ МВД России, 2023. – 80 с.

*Авторский коллектив:*
*Синещук Ю.И.* (введ., гл. 1–3, закл.); *Родин В.Н.*, *Саратов Д.Н.* (гл. 1), *Локнов А.И.* (гл. 3)

ISBN 978-5-91837-677-5

Учебное пособие предназначено для изучения учебного модуля «Организационно-правовые основы технической защиты конфиденциальной информации» для обучающихся по программе дополнительной профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации» руководителей структурных подразделений (включая государственных гражданских служащих) и специалистов, работающих в области технической защиты конфиденциальной информации, реализуемой в Санкт-Петербургском университете МВД России. Может быть использовано курсантами при изучении дисциплин «Теория информационной безопасности и методология защиты информации», «Организационная защита информации», «Техническая защита информации».

**УДК 004.7**
**ББК 32.88**

**Рецензенты**:
**Еськов А. В.**, доктор технических наук, профессор
(Краснодарский университет МВД России);
**Симаков А. А.,** кандидат технических наук, доцент
(Омская академия МВД России)

ISBN 978-5-91837-677-5

## Оглавление

# ВВЕДЕНИЕ

Категория «информационная безопасность» возникла с появлением средств информационных коммуникаций, хранения и обработки информации, с осознанием возможности нанесения ущерба путём воздействия на эти средства, наличие и развитие которых обеспечивает повышение эффективности профессиональной деятельности различных специалистов.

Обеспечение информационной безопасности объектов информатизации МВД России достигается разработкой и реализацией комплекса мероприятий, включающих весь арсенал имеющихся средств защиты во всех структурных элементах и на всех этапах технологического цикла обработки информации, направленных на поддержание состояния защищенности информационных ресурсов. Обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения угроз конфиденциальной информации. Указанные обстоятельства обусловливают значимость информационной составляющей, информационной культуры в структуре профессиональной деятельности любого сотрудника МВД России, предполагающей владение навыками безопасного использования необходимых информационных ресурсов.

Материал учебного пособия направлен на совершенствование и (или) получение новых компетенций, необходимых для осуществления профессиональной деятельности и (или) повышения профессионального уровня обучающихся в области технической защиты информации. В результате освоения модуля обучающийся должен овладеть способностью использовать правовые акты, методические документы, национальные и международные стандарты в рассматриваемой области в своей профессиональной деятельности, определять виды и формы информации, подверженной угрозам. Кроме того, в учебном пособии изложены организационно-правовые основы технической защиты конфиденциальной информации, включая рассмотрение значимости технической защиты конфиденциальной информации в системе мероприятий защиты информации. Особое внимание уделено анализу государственных систем защиты информации, выявлению места и роли информационной безопасности в системе обеспечения национальной безопасности, классификации информации, подлежащей защите в соответствии с законодательством Российской Федерации.

Наличие соответствующего образования подразумевает обладание базовыми понятиями в области информационных систем и технологий, их достоинств и недостатков. Поэтому в учебном пособии представлен материал с учётом развития у обучающегося знаний, умений и навыков, которые позволят сформировать компетенции для его нового вида профессиональной деятельности и решения задач по организации технической защиты информации.

# Глава 1. ОБЩИЕ ВОПРОСЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

## 1.1. Информация как объект защиты

Практическая реализация регулирования в какой-либо области общественных отношений становится невозможной, если не определить объект, по отношению к которому такое регулирование осуществляется. Единым объектом для рассматриваемой сферы является информация. Первоисточником данного термина является латинское слово *informatio* — изложение, истолкование, разъяснение.

В различных областях приводятся определения, решающие задачи направления.

Информация — обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления.

Информация — это результат отражения и обработки в человеческом сознании многообразия внутреннего и окружающего мира, это сведения об окружающих человека предметах, явлениях природы, деятельности других людей и т. д., а также сведения о его внутреннем состоянии. Сведения, которыми человек обменивается через машину с другим человеком или с машиной, и являются предметом защиты в автоматизированной системе.

Информация — универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и мнений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения.

Существует также целый ряд кратких определений, которые невозможно использовать применительно к потребностям юридической науки, однако они в определенной мере характеризуют информацию как общенаучную категорию, как «универсальную субстанцию»:

Общее, целостное понимание информации определяет ее в двух общих направлениях (парадигмах):

– неотъемлемое свойство материи;

– неотъемлемая составляющая самоуправляемых (технических, биологических, социальных) систем.

В федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» *информация* определяется как *сведения (сообщения, данные) независимо от формы их представления.*

В любом случае во всех аспектах для человека главное то, что информация необходима для познания мира, является «продуктом научного познания», средством изучения реальной действительности и интеллектуального развития общества цивилизации в целом.

Несмотря на то, что интуитивно информация понимается давно, только в наше время все более явно стало пониматься ее значение. Ценность информа-

ции столь значительно выросла, что ее ставят наряду с обычными овеществленными продуктами. Это привело к введению понятия информационного ресурса (ИР), который носит стратегический характер в реализации процессов управления и обеспечения всех сфер жизнедеятельности государства.

Закон об информации, информационных технологиях и защите информации трактует понятие «информационные ресурсы» следующим образом: отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных других информационных системах).

Отметим, что параметры ресурсов и информации отличаются, хотя и близки между собой. Ресурсы — это, фактически, информация на носителях информации и, следовательно, с точки зрения обеспечения безопасности информации защите подлежат именно ее носители.

Качество принятия информационных решений в существенной мере зависит от свойств информационных ресурсов, используемых при решении конкретных задач (проблем).

Важным свойством, качественной характеристикой информации является ее субъективная ценность, т. е. значимость для конкретного субъекта.

Под ценностью информации понимается ее свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженные в стоимостном, временном либо ином эквиваленте.

Далеко не всегда возможно и нужно давать денежную оценку ценности информации. Например, оценка личной информации, политической информации или военной информации не всегда разумна в денежном исчислении. В этом случае предпочтительнее использовать подход, связанный со сравнением ценности отдельных информационных элементов между собой и введением порядковой шкалы ценностей. Всю информацию сравнивают экспертным путем и относят к различным уровням (классам) ценности. Более высокий класс имеет более высокую ценность и поэтому требования по его защите от несанкционированного доступа более высокие.

Ценность информации порождает интересы потенциальных нарушителей информационной безопасности (конкурентов, противников, преступников и др.) к негативным действиям с информацией, систему угроз по нанесению ущерба её владельцам.

Проявления возможного ущерба могут быть различны:

– моральный и материальный ущерб деловой репутации организации;

– моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

– материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

– материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

– материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

– моральный и материальный ущерб от дезорганизации деятельности организации;

– материальный и моральный ущерб от нарушения международных отношений.

В общем случае ущерб может быть причинен каким-либо субъектом, а также явиться следствием, не зависящим от субъекта проявлений (например, стихийных или случайных обстоятельств, непреднамеренных действий).

Поэтому при классификации угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права, определяющего состав преступления.

Вот некоторые примеры составов преступления, определяемых Уголовным кодексом Российской Федерации:

– копирование компьютерной информации — повторение и устойчивое запечатление информации на машинном или ином носителе;

– уничтожение компьютерной информации — стирание ее в памяти ЭВМ;

– модификация компьютерной информации — внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных;

– блокирование компьютерной информации — искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением;

– несанкционированное уничтожение, блокирование модификация, копирование информации — любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

Обман (отрицание подлинности, навязывание ложной информации) — умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Обобщая изложенное, можно утверждать, что угрозами безопасности информации являются:

– хищение (копирование) информации;
– уничтожение информации;
– модификация (искажение) информации;
– нарушение доступности (блокирование) информации;
– отрицание подлинности информации;
– навязывание ложной информации.

Реализация любой из угроз может привести к нарушению базовых свойств, характеризующих состояние информационной безопасности: конфиденциальности, целостности или доступности.

Безопасность информации — состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

Конфиденциальность информации — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Целостность информации — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность информации — состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Для защиты информации затрачиваются определенные силы и средства, а для этого надо знать, какие потери мы понесем при реализации различных видов угроз (денежные, время на восстановление системы и т. п.)

Рассматривая место новых информационных технологий и возможность их использования в управлении, необходимо отметить, что *основным ресурсом автоматизированной системы управления является информация*, а главным ее назначением — сбор, обработка, хранение и использование этой информации в системах управления. Основной задачей противника является воздействие на систему управления противоборствующей стороны. Вывести из строя систему управления означает добиться успеха в реализации своих действий. Следовательно, в современных условиях информация — основной объект атаки противника (рис. 1.1).

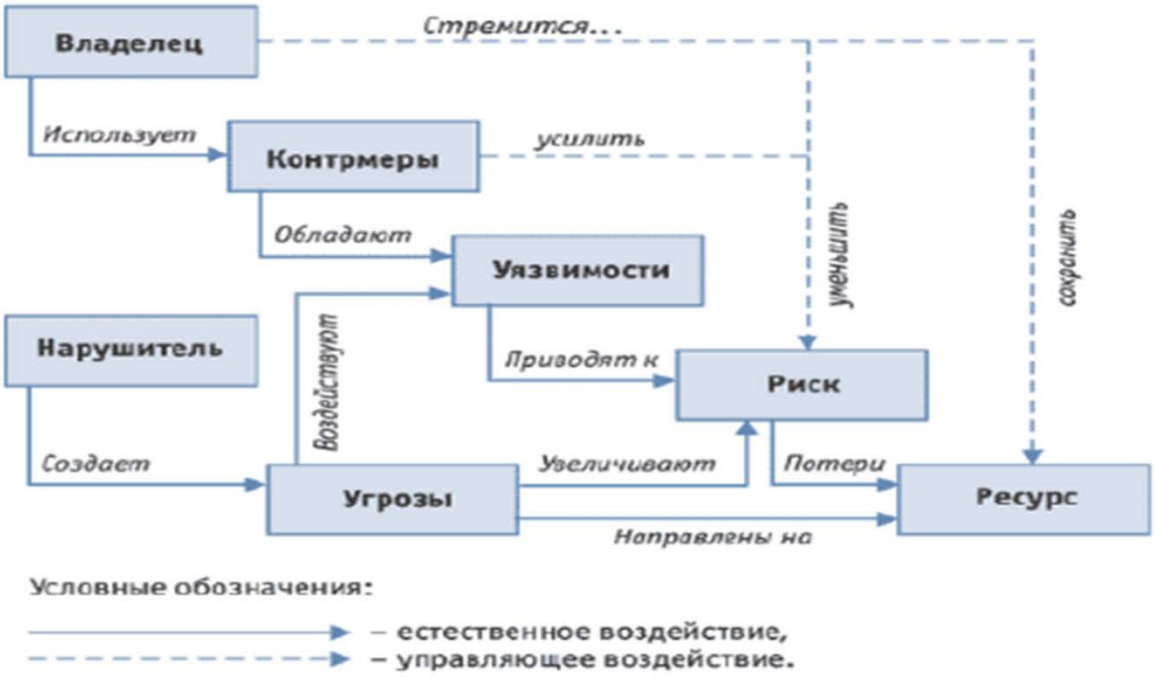


*Рис. 1.1. Таксономическая модель защиты информации*

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Ясно, что в денежном выражении затраты на защиту не должны превышать возможные потери, при этом защищать необходимо не всю информацию, а только ту, которая имеет цену

В настоящее время из многообразия информации выделяют более двадцати видов открытой информации по ее отраслевой принадлежности и востре-

бованности в обществе (научная, техническая, правовая, медицинская, биржевая, финансовая, коммерческая, социальная и др.).

В современном законодательстве упоминается более тридцати видов тайны, которые выступают в виде прямых ограничений при реализации информационных прав и свобод (рис. 1.2).

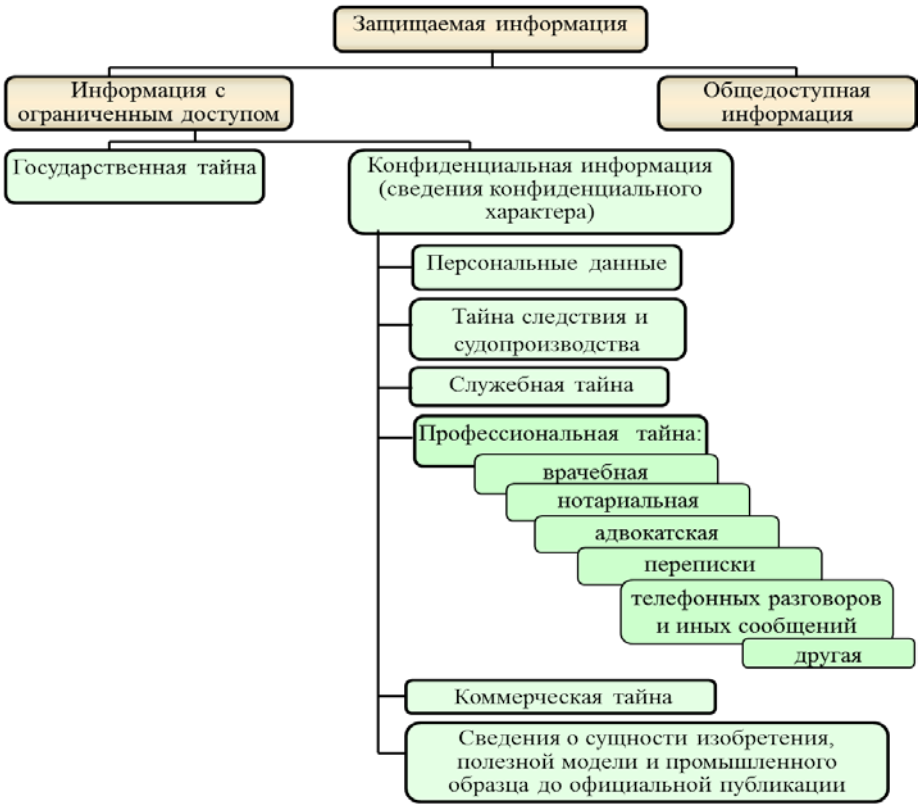


*Рис. 1.2. Классификация защищаемой информации*

При определении права на информацию в качестве самостоятельного объекта защиты для государства было бы безнадежно пытаться защищать всю информацию. Для более эффективного решения задач защиты информации предлагается в качестве объекта защиты избрать лишь информацию с ограниченным доступом и права на нее.

## 1.2. Цели и задачи технической защиты конфиденциальной информации

Техническая защита информации — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Техническая защита конфиденциальной информации представляет собою комплекс мероприятий и (или) услуг по её защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воз-

действий на такую информацию в целях её уничтожения, искажения или блокирования доступа к ней.

Важно обратить внимание, что техническая защита — это не только защита от утечки информации по техническим каналам, но и защита от несанкционированного доступа (НСД), от математического воздействия, от вредоносных программ и т. п.

*Цель* технической защиты информации — обеспечение целостности, конфиденциальности и доступности защищаемой информации.

*Основные задачи* технической защиты информации:

– предотвращение утечки информации через технические каналы утечки информации;

– предотвращение несанкционированного доступа к информации.

Техническая защита информации — одна из основных составляющих комплекса мер по защите информации. Этот комплекс включает нормативно-правовые документы, организационные и технические меры, направленные на обеспечение безопасности конфиденциальной информации.

Для обеспечения эффективной технической защиты информации необходимо определить:

✓ что защищать техническими средствами в данной организации, здании, помещении;

✓ каким угрозам подвергается защищаемая информация со стороны злоумышленников и их технических средств;

✓ какие способы и средства целесообразно применять для обеспечения информационной безопасности с учётом как величины угрозы, так и затрат на её предотвращение;

✓ как организовать и реализовать техническую защиту информации в организации.

Без этих знаний защита информации может проводиться в форме круговой обороны (при неограниченных ресурсах) или «латания дыр» в более реальном варианте ограниченности средств.

При организации защиты информации, как и других видов защиты, необходимо также знать и учитывать психологические факторы, влияющие на принятие решения руководителем или любым другим ответственным лицом. Это обусловлено тем, что меры по защите имеют превентивную направленность без достаточно достоверных данных о потенциальных угрозах не вообще, а применительно к конкретной организации. Кроме того, последствия скрытого хищения информации проявляются спустя некоторое время, когда порой бывает достаточно трудно выявить истинную причину ухудшения финансового положения фирмы или появления у конкурента идентичной продукции. Эти факторы не способствуют психологической готовности руководителя на достаточно большие затраты на защиту информации. Тем не менее, мировой опыт организации защиты информации подтверждает, что на информационную безопасность фирмы вынуждены выделять порядка 10–20 % от общей прибыли. Поскольку значительную часть расходов на защиту информации составляют за-

траты на покупку и эксплуатацию средств защиты, то методология инженерно-технической защиты информации должна обеспечивать возможность рационального выбора средств защиты информации.

Однако выбор средств защиты информации с ориентацией на рекламные данные чреват крупными ошибками, так как в рекламе фирмы-производители не указывают недостатки и преувеличивают достоинства своей продукции. Нужны более глубокие знания о принципах работы и возможностях тех или иных технических средств защиты информации.

Таким образом, при решении задач защиты информации объективно существует необходимость учёта большого числа различных факторов, что не удаётся, как правило, сделать на основе здравого смысла. Поэтому основы инженерно-технической защиты информации должны содержать как теоретические знания, так и методические рекомендации, обеспечивающие решение этих задач.

## 1.3. Принципы технической защиты информации

Так как органам безопасности, занимающимся защитой информации, противостоит разведка с мощным аппаратом и средствами, находящимися на острие научно-технического прогресса, то возможности способов и средств защиты не должны, по крайней мере, уступать возможностям разведки. Исходя из этих исходных положений основу защиты информации должны составлять, аналогичные принципам добывания информации, а именно:

– непрерывность защиты информации, характеризующаяся постоянной готовностью системы защиты в любое время к отражению угроз информационной безопасности;

– активность, предусматривающая прогнозирование действий злоумышленника, разработку и реализацию опережающих мер по защите;

– скрытность, исключающая ознакомление посторонних лиц со средствами и технологией защиты информации;

– целеустремлённость, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценной информации;

– комплексное использование различных способов и средств защиты информации, позволяющее компенсировать недостатки одних достоинствами других.

Эти принципы хотя и не содержат конкретных рекомендаций, однако определяют общие требования к способам и средствам защиты информации.

Следующая группа принципов характеризует основные профессиональные подходы к организации защиты информации, обеспечивает рациональный уровень её защиты и позволяет сократить затраты. Эта группа включает следующие принципы:

– соответствие уровня защиты ценности информации;

– гибкость защиты;

– многозональность защиты, предусматривающая размещение источников информации в зонах с контролируемым уровнем её безопасности;

– многорубежность защиты информации на пути движения злоумышленника или распространения носителя.

Первый принцип определяет экономическую целесообразность применения тех или иных средств мер защиты. Он заключается в том, что затраты на защиту информации не должны превышать цену защищаемой информации.

Так как цена информации — величина переменная, зависящая как от источника информации, так и от времени, то во избежание неоправданных расходов защита информации должны быть гибкой. Гибкость защиты проявляется в возможности изменения степени защищённости в соответствии с изменившимися требованиями к информационной безопасности.

Требуемый уровень информационной безопасности достигается многозональностью и многорубежностью защиты. Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к источникам информации и реализуется путём разделения пространства, занимаемого объектом защиты (организацией, предприятием, фирмой или любой другой государственной или коммерческой структурой) на так называемые контролируемые зоны. Типовыми зонами являются:

– территория, занимаемая объектом защиты и ограниченная забором или условной внешней границей;

– здание на территории;

– коридор или его часть;

– помещение;

– шкаф, сейф, хранилище.

Зоны могут быть независимыми (здания, помещения), пересекающимися и вложенными (сейф в комнате, комната в здании, здание на территории).

С целью воспрепятствования проникновению злоумышленника в зону на её границе создаются, как правило, один или несколько рубежей защиты. Рубежи защиты создаются и внутри зоны на пути возможного движения злоумышленника или распространения иных носителей, прежде всего электромагнитных и акустических полей. Например, для защиты акустической информации от прослушивания в помещении может быть установлен рубеж защиты в виде акустического экрана.

Каждая зона характеризуется уровнем безопасности находящейся в ней информации. Информационная безопасность в зоне зависит:

– от расстояния от источника информации (сигнала) до злоумышленника или его средств добывания информации;

– количества и уровня защиты рубежей на пути движения злоумышленника или распространения иного носителя информации (например поля);

– эффективности способов и средств управления допуском людей и автотранспорта в зону;

– мер по защите информации внутри зоны.

Чем больше удалённость источника информации от места нахождения злоумышленника или его средства добывания информации и чем больше рубежей защиты, тем больше время движения злоумышленника к источнику и ослабление энергии носителя в виде поля или электрического тока. Количество и пространственное расположение зон и рубежей выбирается таким образом, чтобы обеспечить требуемый уровень информационной безопасности как от внешних (вне территории организации), так и внутренних (проникших на территорию злоумышленников или сотрудников) факторов атаки на защищаемый объект. Чем более ценной является информация, тем большим количеством рубежей и зон целесообразно окружить её источник и тогда тем сложнее злоумышленнику обеспечить разведывательный контакт с её носителями.

Рассмотренные выше принципы относятся к защите информации в целом. При построении системы защиты информации нужно учитывать также следующие принципы:

– минимизация дополнительных задач и требований к сотрудникам организации, вызванных мерами по защите информации;

– надёжность в работе технических средств системы, исключающая как нереагирование на угрозы (пропуски угроз) информационной безопасности, так и ложные реакции при их отсутствии;

– ограниченный и контролируемый доступ к элементам системы обеспечения информационной безопасности;

– непрерывность работы системы в любых условиях функционирования объекта защиты, в том числе, например, кратковременном отключении электроэнергии;

– адаптируемость (приспособляемость) системы к изменениям окружающей среды.

Смысл указанных принципов очевиден, но следует остановиться подробнее на последнем. Дело в том, что закрытая информация о способах и средствах защиты информации в конкретной организации со временем становится известной всё большему числу людей, в результате чего увеличивается вероятность попадания этой информации к злоумышленнику. Поэтому целесообразно производить изменения в структуре системы защиты информации периодически или при появлении достаточно реальной возможности утечки информации о системе защиты, например, при внезапном увольнении информированного сотрудника службы безопасности.

## 1.4. Требования к технической защите информации

Документация государственного регулирования устанавливает минимальные требования защиты от несанкционированного доступа к данным. Выполнение требований регулятора по технической защите информации — Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России) обязательно:

– при оказании услуг информационной безопасности (ТЗКИ, КрЗИ);

– выполнении обязанностей оператора персональных данных (ПНд);
– передаче информации посредством сети Интернет.

Требования ФСТЭК России по технической защите информации распространяются:

– на программное обеспечения и оборудование;
– внешние носители;
– средства связи и шифровки/дешифровки данных;
– операционные системы;
– прочие технические средства хранения, обработки, передачи сведений;
– персональные данные;
– специалистов по обеспечению информационной безопасности.

Так, в состав мер по защите персональных данных согласно требованиям ФСТЭК России входят:

– использование системы идентификации и аутентификации (авторизации) субъектов, имеющих доступ к ПНд, и объектов ПНд;
– возможность ограничения и управления правами доступа к персональной информации;
– физическая и программная защита носителей информации;
– регистрация событий безопасности и ведение их журнала;
– применение средств антивирусной защиты;
– регулярный контроль защищенности ПНд;
– обнаружение и предотвращение вторжений, несанкционированного доступа;
– обеспечение доступности хранимых сведений, их и информационной системы, базы данных доступности;
– соблюдение требований по защите среды виртуализации, технических средств, информационной системы (ИС), ее средств, каналов и линий связи и передачи данных.

Также требованиями ФСТЭК России по защите персональных данных предусмотрено наличие возможности управления конфигурацией ИС, своевременного выявления инцидентов, способных привести к сбоям в работе ИС, возникновению угроз безопасности ПНд.

Требования ФСТЭК России к специалистам по защите информации включают в себя понимание:

– основных законодательных и нормативных актов в области информационной безопасности и защиты персональных данных;
– в области сертификации средств защиты информации;
– о государственной системе противодействия иностранным техническим разведкам.

К профессиональным знаниям специалистов относятся:

– подготовка в части работы с каналами и линиями связи (предотвращение утечки информации);
– ориентация в сфере комплексных средств защиты информации (СЗИ);
– понимание основ методологии построения СЗИ;

– умение работать со средствами контроля защищенности баз данных (БД) и т. д.

Требования ФСТЭК по защите конфиденциальной информации направлены на исключение неправомерного доступа, копирования, передачи или распространения сведений. Для обеспечения требований по безопасности конфиденциальной информации проводится оценка возможных уязвимостей ИС для внешних и внутренних нарушителей, возможных средств реализации этих уязвимостей.

## 1.5. Роль и место технической защиты в системе мероприятий по защите информации

Многообразие функций и задач, решаемых предприятиями различных сфер деятельности и организационно-правовых форм, требует постоянного совершенствования системы защиты конфиденциальной информации, принятия новых нормативных актов, методических документов, инструкций и руководства для работников предприятия.

Этим обусловлено вполне объяснимое стремление руководителей организаций и предприятий создать и на необходимом уровне поддерживать эффективную систему защиты информации, способную в каждом конкретном случае с учетом специфики деятельности предприятия определить необходимую совокупность сил и средств, а также мероприятий, используемых при решении задач по защите информации.

Федеральный закон «Об информации, информационных технологиях и защите информации» определяет *защиту информации как принятие правовых, организационных и технических мер*, направленных:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа.

Реальный интерес к проблеме защиты информации, проявляемый руководством, на уровне подразделений, отвечающих за работоспособность информационной системы, сменяется на резкое неприятие. Как правило, приводятся следующие аргументы против проведения работ и принятия мер по обеспечению информационной безопасности:

– появление дополнительных ограничений для конечных пользователей и специалистов подразделений обеспечения, затрудняющие использование, эксплуатацию автоматизированной системы организации;

– необходимость дополнительных материальных затрат как на проведение таких работ, так и на расширение штата специалистов, занимающихся проблемой информационной безопасности.

Экономия на информационной безопасности может выражаться в различных формах, крайними из которых являются:

– принятие только организационных мер обеспечения безопасности информации;

– использование только дополнительных технических средств защиты информации (ТСЗИ).

В первом случае, как правило, разрабатываются многочисленные инструкции, приказы и положения, призванные в критическую минуту переложить ответственность с людей, издающих эти документы, на конкретных исполнителей. Естественно, что требования таких документов (при отсутствии соответствующей технической поддержки) затрудняют повседневную деятельность сотрудников организации и, как правило, не выполняются.

Во втором случае приобретаются и устанавливаются дополнительные ТСЗИ. Применение ТСЗИ без соответствующей организационной поддержки также неэффективно в связи с тем, что без установленных правил обработки информации применение любых ТСЗИ только усиливает существующий беспорядок.

Обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий.

В целях определения сущности и содержания понятия «обеспечение информационной безопасности» собственно информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, которые в первую очередь характеризуются наличием информационной инфраструктуры и информации. По-иному, информационная безопасность — состояние защищенности объекта безопасности от внешних и внутренних угроз.

Обеспечение информационной безопасности достигается разработкой и реализацией комплекса мероприятий, включающих весь арсенал имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации, направленных на поддержание состояния защищенности всех компонентов информационной системы.

Следовательно, защита информационных ресурсов предприятия включает в себя деятельность руководства, должностных лиц и структурных подразделений предприятия по защите информации от несанкционированного доступа к информации, ее уничтожения, изменения и других опасных воздействий на защищаемую информацию.

Таким образом, обеспечение информационной безопасности есть совокупность деятельности по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности.

Структура понятия «обеспечение информационной безопасности» включает:

1. Деятельность по обеспечению информационной безопасности;

2. Средства осуществления деятельности по обеспечению информационной безопасности;

3. Субъекты обеспечения информационной безопасности.

Деятельность по обеспечению информационной безопасности — это комплекс планируемых и проводимых в целях защиты информационных ресурсов мероприятий, направленных на ликвидацию угроз информационной безопасности и минимизацию возможного ущерба, который может быть нанесен объекту безопасности вследствие их реализации.

Под субъектами обеспечения информационной безопасности понимаются государственные органы, предприятия, должностные лица, структурные подразделения, принимающие непосредственное участие в организации и проведении мероприятий по обеспечению информационной безопасности.

Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, — совокупность сил и средств, используемых для организации защиты информации.

Предприятия, работающие с конфиденциальной информацией и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации. Данные подразделения и должности являются органами защиты информации.

Чтобы добиться максимальной эффективности при решении задач защиты информации, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необходимо использовать имеющиеся на предприятии средства защиты информации.

Средства (в широком смысле), с помощью которых достигаются цели деятельности по обеспечению информационной безопасности — это системы, объекты, способы, методы и иные механизмы непосредственного решения задач обеспечения информационной безопасности. Они представляют собой совокупность правовых, организационных и технических методов обеспечения информационной безопасности. Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.

Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют методы защиты информации, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.

Методы защиты информации — это применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.

Методы защиты информации с точки зрения их теоретической основы и практического использования взаимосвязаны. Правовые методы регламенти-

руют и всесторонне нормативно регулируют деятельность по защите информации, выделяя прежде всего ее организационные направления. Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которого зависит от применяемых методов технического и экономического характера.

Наибольший эффект достигается тогда, когда все используемые средства, методы и меры (мероприятия) объединяются в единый целостный механизм – систему защиты информации (СЗИ), создаваемую на соответствующей нормативно-методической основе и отражающей все направления и специфику деятельности МВД России. При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

Под системой защиты информации понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.

При создании системы защиты информации в первую очередь учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. В соответствии с названными приоритетами формируется перечень возможных угроз информации, подлежащей защите, и определяются конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна быть:

– централизованной — обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;

– плановой — объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;

– конкретной и целенаправленной — рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;

– активной — обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

– надежной и универсальной — охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.

Таким образом, задача защиты информации успешно реализуется только при системном подходе к ее решению.

С этой целью предложена следующая классификация методов защиты информации:

– по классу решаемых задач — технические, программные, организационные;

– по виду решаемых задач — резервирование, введение избыточности, регулирование доступа, регулирование использования, защитные преобразования, контроль, регистрация, уничтожение, сигнализация, реагирование;

– по функциональному назначению — решение задач защиты самостоятельными средствами, решение задач защиты в комплексе с другими средствами, управление средствами защиты, обеспечение функционирования механизмов защиты.

По способам осуществления все методы обеспечения безопасности компьютерных систем подразделяют:

на *неформальные* — правовые (законодательные), морально-этические, организационные (административные);

*формальные (технические)* — физические, инженерно-технические, аппаратно-программные.

Формальные методы реализуются соответствующими средствами защиты, а неформальные соответствующими мерами или мероприятиями защиты информации (рис. 1.3).

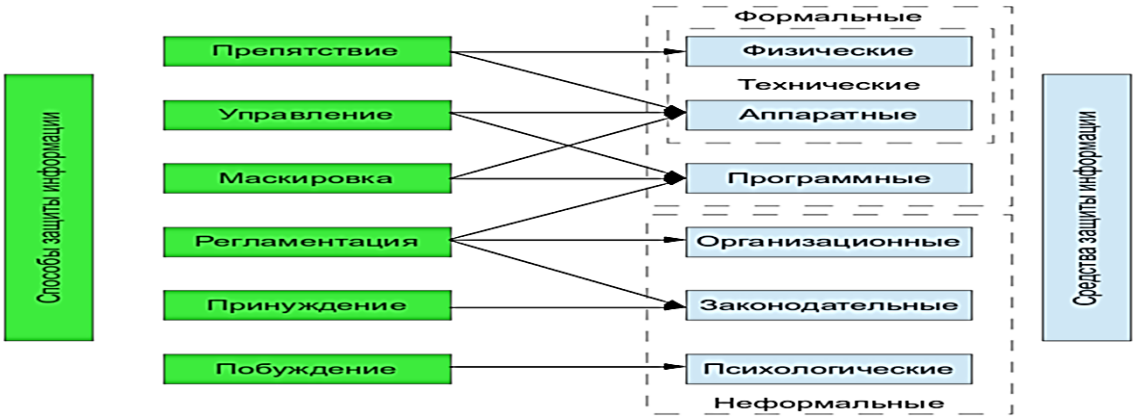


*Рис. 1.3. Способы и средства (меры, мероприятия) защиты информации*

По охвату защитные средства и меры могут быть ориентированы на защиту территории фирмы, зданий, отдельных (выделенных) помещений, конкретных видов аппаратуры или технических средств и систем или отдельных элементов зданий, помещений, аппаратуры, опасных с точки зрения несанкционированного доступа к ним или оборудования каналов утечки информации.

Применение защитных мер можно рассматривать и в пространственном плане. Так, например, известно, что распространение (разглашение, утечка или несанкционированный доступ) осуществляется от источника информации через информационную среду к злоумышленнику.

Мероприятия охватывают целый ряд аспектов законодательного, организационного и программно-технического характера. Для каждого из них формулируется ряд задач, выполнение которых необходимо для защиты информации. Перечислим самые общие из них.

*В нормативно-законодательном аспекте* необходимо решение следующих задач:

– определение круга нормативных документов международного, федерального и отраслевого уровня, применение которых требуется при проектировании и реализации системы информационной безопасности;

– определение на основе нормативных документов требований по категорированию информации;

– определение на основе нормативных документов базовых требований к системе информационной безопасности и ее компонентам.

*В организационном аспекте:*

– определение соответствия структурируемой и защищаемой информации подсистемам и ресурсам информационной системы, в которых производится хранение, обработка и передача информации конечному пользователю (должно быть организовано ведение реестра ресурсов, содержащих информацию, значимую по критериям конфиденциальности, целостности и доступности);

– определения набора служб, обеспечивающих доступ к информационным ресурсам системы (необходима выработка и согласование типовых профилей пользователей, ведение реестра таких профилей);

– формирования политики безопасности, включающей описание границ и способов контроля безопасного состояния системы, условия и правила доступа различных пользователей к ресурсам системы, мониторинга деятельности пользователей.

*В процедурном аспекте:*

– организация физической защиты помещений и компонентов информационной системы, включая сети и телекоммуникационные устройства;

– обеспечение решения задач информационной безопасности при управлении персоналом;

– формирование, утверждение и реализация плана реагирования на нарушения режима безопасности;

– внесение дополнений, связанных со спецификой ликвидации последствий несанкционированного доступа, в план восстановительных работ.

*В программно-техническом аспекте:*

– обеспечение архитектурной и инфраструктурной полноты решений, связанных с хранением, обработкой и передачей конфиденциальной информации;

– обеспечение проектной и реализационной непротиворечивости механизмов безопасности по отношению к функционированию информационной системы в целом;

– выработка и реализация проектных и программно-аппаратных решений по механизмам безопасности.

Мероприятия по защите информации должны исключать:

– выход излучений электромагнитного и акустического полей, а также наводок в сетях питания, кабельных линиях, заземлении, радио- и телефонных сетях за пределы контролируемой зоны;

– доступ в помещение, где осуществляется обработка информации, а также визуально-оптические возможности съема информации;

– работу специальных устройств ведения разведки, которые могут находиться в строительных конструкциях помещений и предметах их интерьера, а также внутри самого помещения или непосредственно в средствах обработки и передачи информации;

– перехват информации из каналов передачи данных;

– несанкционированный доступ к информационным ресурсам;

– воздействие излучений, приводящих к разрушению информации.

Множество и разнообразие возможных методов, мероприятий и средств защиты информации определяется прежде всего возможными *способами воздействия на дестабилизирующие факторы или порождающие их причины*, причем воздействия в направлении, способствующем повышению значений показателей защищенности или (по крайней мере) сохранению прежних (ранее достигнутых) их значений.

Меры (мероприятия) безопасности, средства и способы защиты информации можно рассматривать как последовательность барьеров или рубежей защиты информации. Для того чтобы добраться до защищаемой информации, нужно последовательно преодолеть несколько рубежей защиты (рис. 1.4).


*Рис. 1.4. Система мероприятий (рубежей) защиты информации*

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые определяются состоянием устремленности нарушителя либо действиями конкурента, направленными на овладение информацией, подлежащей защите. Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

*Вопросы и задания для самоконтроля*

1. Охарактеризуйте информацию как объект защиты.
2. Какие принципы положены в основу организации технической защиты информации?
3. Обоснуйте место и роль технической защиты конфиденциальной информации в системе в системе мероприятий защиты информации.
4. Сформулируйте цели и задачи технической защиты конфиденциальной информации.

# Глава 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

## 2.1. Вопросы информационной безопасности в перечне национальных интересов Российской Федерации

В настоящее время базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития Российской Федерации на долгосрочную перспективу, является *Стратегия национальной безопасности Российской Федерации*[1] (далее — Стратегия).

Стратегия (др. греч. στρατηγία – «искусство полководца») — общий, не детализированный план какой-либо деятельности, охватывающий длительный период времени, способ достижения сложной цели. Стратегия как способ действий становится необходимой в ситуации, когда для прямого достижения основной цели недостаточно наличных ресурсов. Задачей стратегии является эффективное использование наличных ресурсов для достижения основной цели. Стратегия достигает основной цели через решение промежуточных тактических задач по критерию «ресурсы-цель», таким образом, стратегия – интегрированная модель действий, предназначенных для достижения целей предприятия; образ действий в виде взаимосвязанного комплекса управленческих решений, обеспечивающих достижение поставленных целей.

*Необходимость разработки и совершенствования стратегии вызвана*:

1) обострением межгосударственных противоречий, связанных с неравномерностью их развития и углублением разрыва между уровнем благосостояния стран;

2) уязвимостью всех членов международного сообщества перед лицом новых вызовов и угроз;

3) укреплением новых центров экономического роста и политического влияния и складывающейся качественно новой геополитической ситуацией;

4) несостоятельностью глобальной и отдельных региональных систем безопасности;

5) несовершенством правовых инструментов и механизмов, создающих угрозу обеспечению международной безопасности;

6) необходимостью решения важных внутренних вопросов в области здравоохранения, образования, науки, экологии, культуры, а также повышения уровня благосостояния граждан и экономического роста.

*Стратегия* основана на неразрывной взаимосвязи и взаимозависимости национальной безопасности Российской Федерации и социально-экономического развития страны.

[1] Утв. указом Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

Правовую основу Стратегии составляют Конституция Российской Федерации, федеральные законы от 28 декабря 2010 г. № 390-ФЗ «О безопасности», от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», другие федеральные законы, нормативные правовые акты Президента Российской Федерации.

Конституция является основным источником права в области обеспечения безопасности в России.

Закон РФ от 28 декабря 2010 г. № 390-ФЗ «О безопасности» определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее — безопасность, национальная безопасность), полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.

Стратегия содержит следующие основные разделы:

I. Общие положения.

II. Россия в современном мире: тенденции и возможности.

III. Национальные интересы Российской Федерации и стратегические национальные приоритеты.

IV. Обеспечение национальной безопасности:

- ✓ Сбережение народа России и развитие человеческого потенциала.
- ✓ Оборона страны.
- ✓ Государственная и общественная безопасность.
- ✓ *Информационная безопасность.*
- ✓ Экономическая безопасность.
- ✓ Научно-технологическое развитие.
- ✓ Экологическая безопасность и рациональное природопользование.
- ✓ Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти.
- ✓ Стратегическая стабильность и взаимовыгодное международное сотрудничество.

V. Организационные основы и механизмы реализации Стратегии.

*Стратегия национальной безопасности Российской Федерации* — это базовый документ стратегического планирования, *определяющий национальные интересы и стратегические национальные приоритеты Российской Федерации, цели и задачи государственной политики* в области обеспечения национальной безопасности и устойчивого развития Российской Федерации на долгосрочную перспективу.

Основная задача Стратегии состоит *в обеспечении национальной безопасности* — реализация органами публичной власти во взаимодействии с институтами гражданского общества и организациями политических, правовых, воен-

ных, социально-экономических, *информационных*, организационных и иных мер, направленных на противодействие угрозам национальной безопасности.

С учетом долгосрочных тенденций развития ситуации в Российской Федерации и в мире ее *национальными интересами* на современном этапе являются:

1) сбережение народа России, развитие человеческого потенциала, повышение качества жизни и благосостояния граждан;

2) защита конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации, укрепление обороны страны;

3) поддержание гражданского мира и согласия в стране, укрепление законности, искоренение коррупции, защита граждан и всех форм собственности от противоправных посягательств, развитие механизмов взаимодействия государства и гражданского общества;

4) *развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия;*

5) устойчивое развитие российской экономики на новой технологической основе;

6) охрана окружающей среды, сохранение природных ресурсов и рациональное природопользование, адаптация к изменениям климата;

7) укрепление традиционных российских духовно-нравственных ценностей, сохранение культурного и исторического наследия народа России;

8) поддержание стратегической стабильности, укрепление мира и безопасности, правовых основ международных отношений.

Обеспечение и защита национальных интересов Российской Федерации осуществляются за счет концентрации усилий и ресурсов органов публичной власти, организаций и институтов гражданского общества на реализации следующих *стратегических национальных приоритетов*:

1) сбережение народа России и развитие человеческого потенциала;

2) оборона страны;

3) государственная и общественная безопасность;

4) информационная безопасность;

5) экономическая безопасность;

6) научно-технологическое развитие;

7) экологическая безопасность и рациональное природопользование;

8) защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти;

9) стратегическая стабильность и взаимовыгодное международное сотрудничество.

Реализация Стратегии осуществляется на плановой основе путем согласованных действий органов публичной власти, организаций и институтов гражданского общества под руководством Президента Российской Федерации за счет комплексного применения политических, организационных, социально-экономи-

ческих, правовых, *информационных*, военных, специальных и иных мер, разработанных в рамках стратегического планирования в Российской Федерации.

В Стратегии уточнён и конкретизирован ряд понятий теории национальной безопасности:

– национальные интересы Российской Федерации — объективно значимые потребности личности, общества и государства в безопасности и устойчивом развитии;

– *стратегические национальные приоритеты Российской Федерации* — важнейшие направления обеспечения национальной безопасности и устойчивого развития Российской Федерации;

– национальная безопасность Российской Федерации — состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны;

– угроза национальной безопасности — совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам Российской Федерации;

– система обеспечения национальной безопасности (СОНБ) — совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов публичной власти и находящихся в их распоряжении инструментов.

Достижению национальных интересов препятствуют те или иные угрозы. Угроза может быть внешней или внутренней в зависимости от того, где расположен источник опасности. Если опасность исходит от другого государства или его граждан, то угроза признается внешней, если же нанесение вреда исходит со стороны сограждан государства, то это внутренняя угроза.

Деление угроз безопасности на эти два вида имеет практическую значимость, хотя в настоящее время воздействие многих угроз носит трансграничный характер. К ним относятся политические, военно-политические или силовые, информационные угрозы интересам и безопасности Российской Федерации, которые совмещают в себе черты внутренних и внешних угроз и, будучи по форме проявления внутренними, по своей сути (по источникам возникновения и стимуляции, возможным участникам и т. д.) являются внешними. Трансграничные угрозы для безопасности Российской Федерации имеют тенденцию к возрастанию.

Основываясь на положениях федерального закона «О безопасности» и Стратегии, можно выделить некоторые элементы структуры национальной безопасности. В Стратегии определены три основных объекта безопасности — личность, общество и государство. Иными словами, личность, общество и государство являются элементами структуры объекта национальной безопасности, а не самой национальной безопасности.

При этом следует различать систему обеспечения национальной безопасности и систему национальной безопасности.

Первая — это система органов, сил, средств, различных организаций, призванных решать задачи по обеспечению национальной безопасности, а вторая-это функциональная система, отражающая процессы взаимодействия национальных интересов и разнообразных форм угроз, возникающих в тех или иных сферах жизнедеятельности государства.

Система национальной безопасности России складывается из совокупности составляющих (видов национальной безопасности), которые должны обеспечивать сбалансированные интересы личности, общества и государства в отношении. К этим составляющим (видам) относятся безопасность в международной, экономической, военной, внутриполитической, информационной, социальной, экологической и других сферах (рис. 2.1).


*Рис. 2.1. Элементы структуры системы национальной безопасности*

При этом одна из ключевых ролей в системе обеспечения национальной безопасности отводится информационной составляющей.

## 2.2. Эволюция места и роли информационной безопасности в системе обеспечения национальной безопасности

На обеспечение национальных интересов Российской Федерации негативное влияние будут оказывать вероятные рецидивы односторонних силовых подходов в международных отношениях, противоречия между основными участниками мировой политики, угроза распространения оружия массового уничтожения и его попадания в руки террористов, а также *совершенствование форм противоправной деятельности в кибернетической и биологической областях, в сфере высоких технологий. Усилится глобальное информационное противоборство,* возрастут угрозы стабильности индустриальных и развивающих-

ся стран мира, их социально-экономическому развитию и демократическим институтам».

Защита информации обеспечивается в любом государстве и в своем развитии проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств ее добывания, правового режима и реальных усилий его по обеспечению защиты информации. Информация, проникая во все сферы деятельности государства, приобретает конкретные политические, материальные и стоимостные выражения. На этом фоне в настоящее время все более актуальный характер приобретает задача обеспечения информационной безопасности России как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

Достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач:

1) формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования;

2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;

3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;

4) создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий;

5) повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети Интернет, иных значимых объектов информационно-коммуникационной инфраструктуры, а также недопущение иностранного контроля за их функционированием.

Информационная сфера становится не только важнейшей сферой международного сотрудничества, но и объектом соперничества. Проблемы в сфере информационных отношений, формирования информационных ресурсов и пользования ими обостряются вследствие политического и экономического противоборства различных государств, имеющего место информационного неравенства. При этом ведется активная работа по вытеснению России с внешнего и внутреннего информационного рынка, вовлечение страны в «информационные войны» в целях нарушения нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов. На фоне всего этого наблюдается  и тенденция получения несанкционированного доступа к информации  закрытого характера и использование ее в целях подрыва безопасности государства (технологии «оранжевых революций и т. п.). Самостоятельный блок информационных угроз представляет стремление отдельных стран к доминированию в мировом информационном пространстве.

Угрозы информационной безопасности в ходе реализации Стратегии предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов информатизации Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности (рис. 2.2).

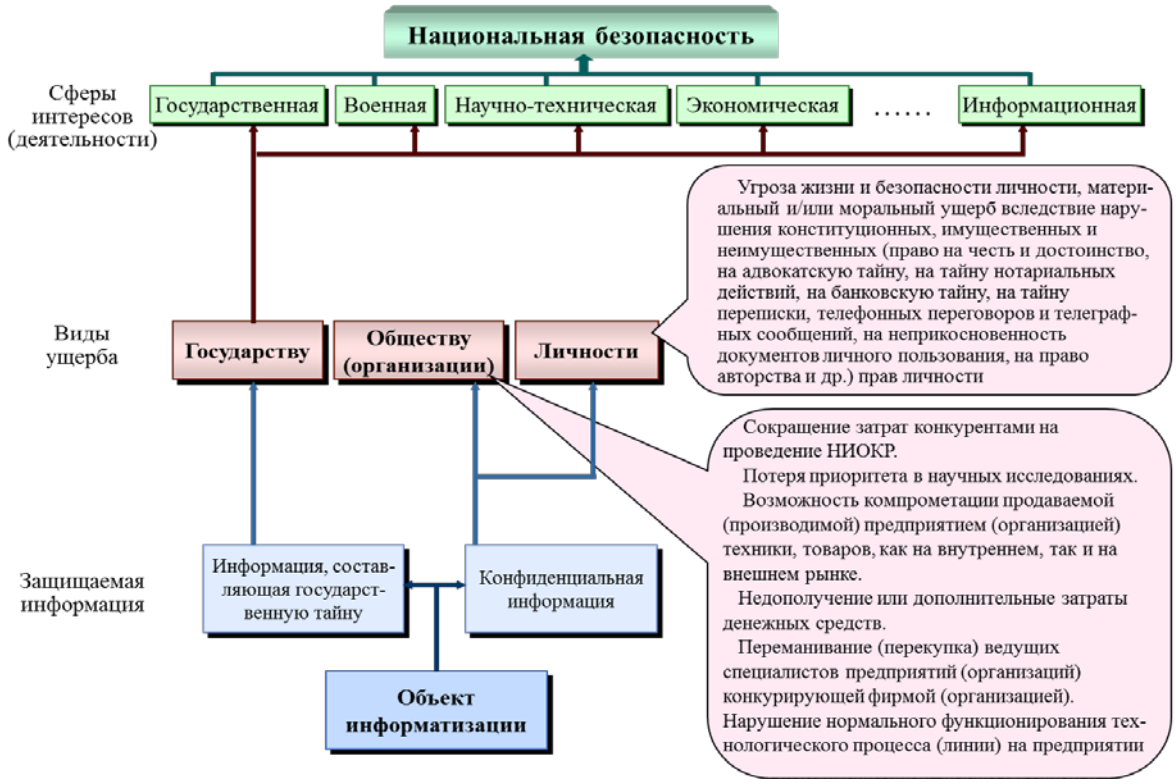


*Рис. 2.2. Роль и влияние средств информатизации на обеспечение национальной безопасности*

Исходя из вышеизложенного, можно заключить, что реализация национальных интересов России возможна только на основе обеспечения ее безопасности в информационной сфере. В этих условиях вопросы информационной безопасности становятся не менее важными, чем вопросы военной безопасности. Информационное воздействие применяется как для обеспечения применения радиоэлектронных средств, так и в качестве идеологического прикрытия при создании необходимого образа справедливости проводимой политики в общественном сознании.

Информационные системы, включающие телекоммуникации, аналитическую и прогнозируемую информацию, не только обеспечивают информационную поддержку функционирования различных сфер жизнедеятельности страны, но и могут оказывать воздействие на состояние безопасности страны в целом.

Поэтому решение задач обеспечения безопасности борьбы в информационной сфере не сводится только к защите каналов и средств передачи информации, охране государственной тайны, правительственной связи и информации и другим вопросам, которые принято рассматривать при анализе совокупности угроз и системы мер по обеспечению информационной безопасности. К вопросам информационной безопасности также относятся безопасность информационных систем управления промышленностью, отраслями, предприятиями, банками.

Необходимо отметить, что угрозы информационной безопасности весьма многообразны, не всегда могут классифицироваться и систематизироваться, поскольку динамика развития науки, технологий, общества и экономики, в целом, постоянно изменяют существующие и создают новые угрозы. К таким угрозам можно отнести международный кибертерроризм, информационно-финансовые атаки и т. д. Угрозы информационной безопасности могут быть направлены как на разрушение любого компонента системы обеспечения национальной безопасности и их взаимосвязи, так и на механизм обеспечения в целом.

Кроме того, влияние угроз в информационной сфере во все возрастающей степени направленно на интересы личности, общества и государства. При этом воздействие на личность в целях снижения активности жизненной позиции все больше осуществляется посредством коммуникационных средств и технологий.

Сложность стоящих перед Россией задач требует выработки сбалансированной стратегии их решения, исходящей из взаимосвязанности проблем национальной безопасности и информационной безопасности.

Новые вызовы и угрозы в информационной сфере (прежде всего кибертерроризм, информационный шпионаж, организованная преступность в информационной сфере, опасность распространения вирусных компьютерных атак на информационно-управляю-щие системы в экономике, и прежде всего в финансовой сфере и т. д.) носят глобальный характер и требуют адекватного ответа для их преодоления.

Всё это в совокупности обусловливает повышение роли и значимости информационной безопасности в обеспечении национальной безопасности, превращая ее в системообразующую основу структуры национальной безопасности (рис. 2.3).

Согласно Стратегии — технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению, образуют средства обеспечения национальной безопасности, что свидетельствует об особой важности информационной составляющей системы обеспечения национальной безопасности.

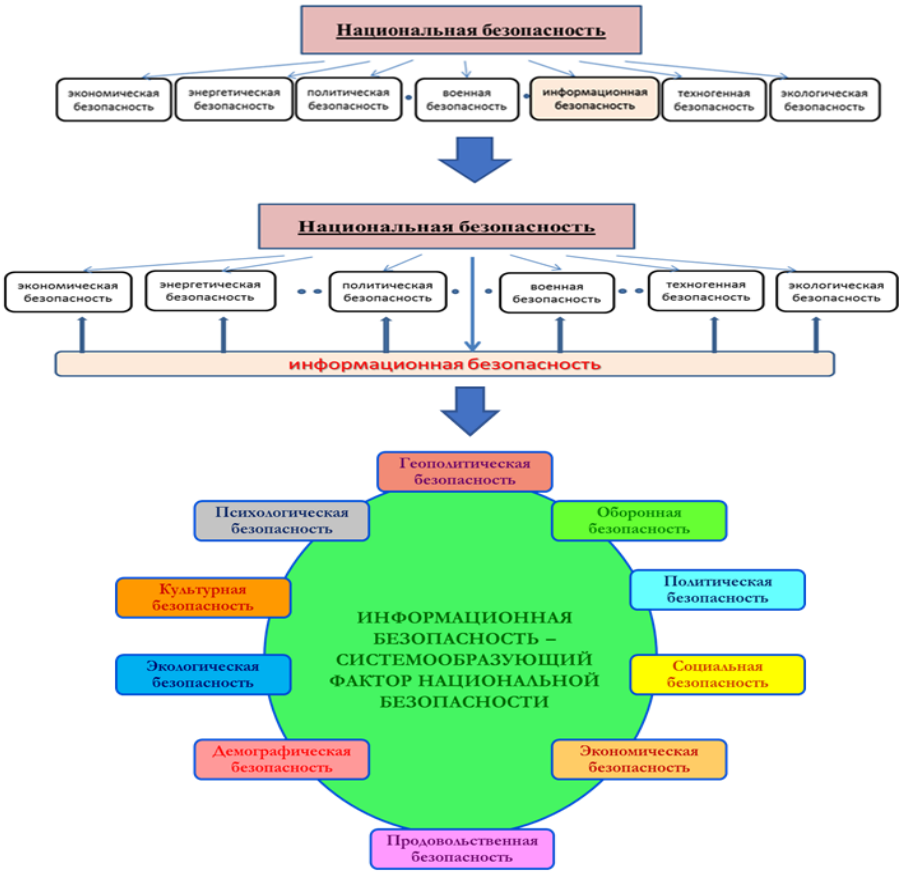


*Рис. 2.3. Эволюция роли и места информационной безопасности в структуре национальной безопасности*

## 2.3. Стратегические цели и направления обеспечения информационной безопасности государства

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства. Проникая во все сферы деятельности государства, информация приобретает конкретное политическое, материальное и стоимостное выражение.

На этом фоне все более актуальный характер приобретают вопросы обеспечения информационной безопасности Российской Федерации как неотъемлемого элемента национальной безопасности, а защита информации превращается в одну из приоритетных задач государства на новом этапе своего развития — этапе формирования информационного общества.

Характерными признаками такого общества является явная обусловленность экономического, социального, научного и всего развития страны широким внедрением новых информационных технологий, обеспечивающих эффективную информатизацию общества. Информатизация личности, общества — это важнейшее, стратегическое направление деятельности государства, определяющее стабильное и безопасное социально-экономическое и политическое

развитие и приоритеты во всех сферах (в том числе в информационной) и видах деятельности в мировом сообществе.

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на информацию как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем защищенности информационных потребностей личности, общества и самого государства, обеспечение их информационной безопасности. При этом *под информационной безопасностью личности, общества, государства и современных автоматизированных и телекоммуникационных систем понимается состояние защищенности информационной среды, соответствующей интересам (потребностям) личности, общества и государства в информационной сфере, при котором обеспечиваются их формирование, использование и возможности развития независимо от наличия внутренних и внешних угроз.*

*Информационная безопасность определяется способностью государства (общества, личности):*

– обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;

– противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

– вырабатывать личностные и групповые навыки и умения безопасного поведения;

– поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Впервые понятие «информационная безопасность» было использовано в 1989 году, в решении Президиума Верховного Совета СССР, которым была организована рабочая комиссия по совершенствованию системы национальной безопасности. Специфика обеспечения информационной безопасности нашла свое отражение в Доктрине информационной безопасности Российской Федерации[1] (далее – Доктрина).

*Доктри́на* — философская, политическая либо правовая теория, религиозная концепция, учение, система воззрений, руководящий теоретический или политический принцип.

Предыдущая доктрина была утверждена соответствующим указом Президента РФ от 9 сентября 2000 г. № Пр-1895. С той поры в сфере информационной безопасности произошли существенные изменения. В частности, на пер-

[1] Утв. указом Президента РФ от 05.12.2016 № 646.

вый план вышла идеология информационной войны: войны за информацию, информационную инфраструктуру и за умы людей. Информационная безопасность стала трактоваться как одна из составляющих информационной войны.

Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии, а также других документов стратегического планирования в указанной сфере, и представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации *в информационной сфере.*

В Доктрине под информационной сферой понимается 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.

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.

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.

Информационная инфраструктура — совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под её юрисдикцией или используемых на основании международных договоров.

В Доктрине используются следующие основные понятия:

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 соци-

ально-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.

Правовую основу Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты президента и правительства.

Доктрина является 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.

Возможности трансграничного оборота информации, на основе применения информационных технологий, 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 (рис. 2.4).

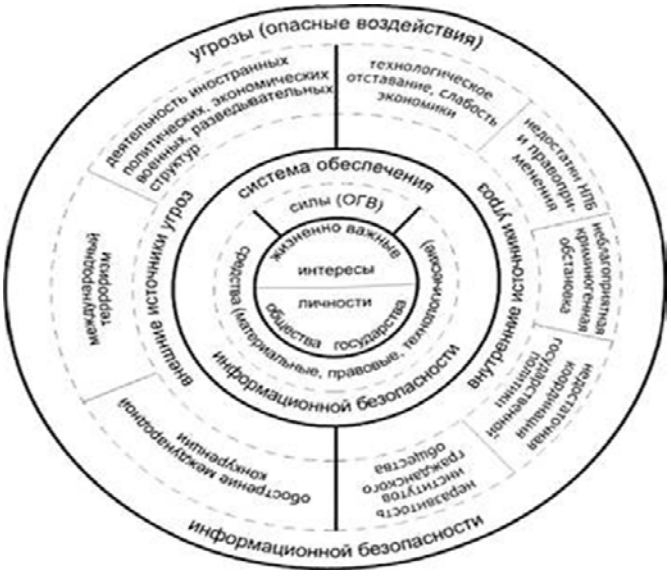


*Рис. 2.4. Угрозы информационной безопасности государства*

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, и 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 привле-

чения 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 характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры.

Информационная безопасность определяется способностью государства, общества, личности:

– обеспечивать с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;

– противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

– вырабатывать личностные и групповые навыки и умения безопасного поведения;

– поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются 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.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

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;

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 ценностей.

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

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.

## 2.4. Система обеспечения информационной безопасности Российской Федерации

Согласно Доктрине информационная безопасность Российской Федерации может быть обеспечена комплексными методами и средствами.

Комплексное обеспечение информационной безопасности — это взаимосвязанный комплекс правовых, организационных, физических, социальных, духовных, информационных, программно-математических и технических методов, мероприятий и средств, обеспечивающих нормальное функционирование государства, его структур, населения, фирм, предприятий как на его территории и в его пространстве, так и в межгосударственных отношениях, независимо от обстановки — мирного труда или военного времени.

Методологию комплексного обеспечения информационной безопасности определяет государственная политика Российской Федерации в этом направлении.

Государственная политика обеспечения информационной безопасности основывается на следующих основных принципах:

– соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права;

– открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

– правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса;

– приоритетное развитие отечественных современных информационных и телекоммуникационных технологий.

Государство в процессе реализации своих функций по обеспечению информационной безопасности в Российской Федерации:

– проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности в Российской Федерации, разрабатывает меры по ее обеспечению;

– организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности;

– поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

– осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

– проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

– способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

– формулирует и реализует государственную информационную политику России;

– организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;

– способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

*Система обеспечения информационной безопасности государства* — совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

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 российским законодательством задач по обеспечению информационной безопасности

Средства обеспечения информационной безопасности — правовые, организационные, технические и другие средства, используемые силами 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.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Россий-

ской Федерации, а также органов местного самоуправления, определяемых законодательством в области обеспечения безопасности.

Основными мероприятиями комплексной системы обеспечения информационной безопасности Российской Федерации являются:

– разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;

– создание условий для реализации прав граждан и общественных объединений на разрешенную законодательством Российской Федерации деятельность в информационной сфере;

– определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

– оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

– координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

– контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

– предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

– развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств;

– повышение конкурентоспособности информационных средств на внутреннем и внешнем рынках;

– организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;

– проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;

– организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;

– защита государственных информационных ресурсов прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

– обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

– совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

– осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации и включает в себя:

– Совет Федерации;
– Государственная думу;
– Правительство;
– Совет Безопасности;
– федеральные органы исполнительной власти (федеральные службы и агентства);
– Центральный банк;
– Военно-промышленную комиссию;
– межведомственные органы, создаваемые президентом и правительством;
– органы исполнительной власти субъектов;
– органы местного самоуправления.

Организационная и функциональная структура системы обеспечения информационной безопасности Российской Федерации представлена на рис. 2.5, 2.6).

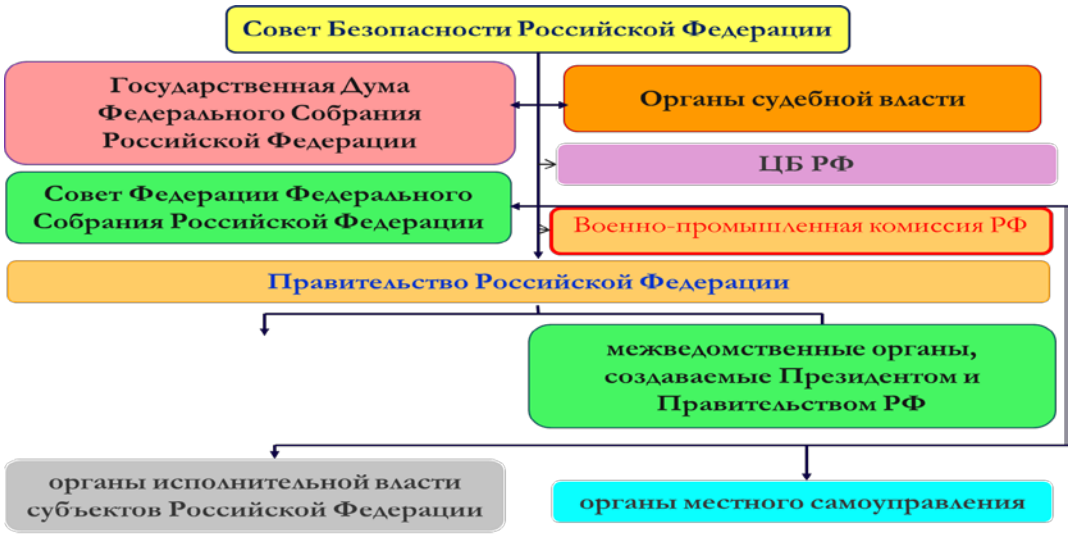


*Рис. 2.5. Организационная структура системы обеспечения информационной безопасности Российской Федерации*


*Рисунок 2.6. Функциональная структура системы обеспечения информационной безопасности Российской Федерации*

*Вопросы и задания для самоконтроля*

1. Дайте краткую характеристику системы обеспечения информационной безопасности Российской Федерации.

2. В каком документе сформулированы национальные интересы и стратегические национальные приоритеты Российской Федерации?

3. Обоснуйте место и роль информационной безопасности в системе обеспечения национальной безопасности.

4. Сформулируйте стратегические цели и направления обеспечения информационной безопасности государства.

# Глава 3. ГОСУДАРСТВЕННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

## 3.1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

1 января 2018 г. вступил в силу федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Многочисленная практика реализации компьютерных(кибер) атак демонстрирует общую тенденцию: каждый опубликованный разбор инцидента и почти каждое тестирование на проникновение демонстрируют наличие в ИТ-инфраструктуре атакованной организации целый комплекс очевидных недостатков: типовые уязвимости веб-приложений, словарные пароли, отсутствие элементарной защиты от перехвата трафика в локальных сетях и т. п. Эти недостатки обнаруживаются практически в каждой организации, независимо от формы собственности, государственной или отраслевой принадлежности.

Такие недостатки в равной степени присутствуют и в коммерческой компании, которая имеет полное право игнорировать проблемы собственной безопасности, и в органе власти, который теоретически должен добросовестно выполнять строгие требования ФСТЭК России в области безопасности информации. Таким образом, если государство ставит перед собой задачу защитить от хакерских атак критически важные информационные системы, то при решении этих задач приходится учитывать несколько аксиом.

Во-первых, из-за организационных и технических ошибок в любой информационной системе в любой момент времени могут присутствовать уязвимости, позволяющие атаковать эту систему. На сегодняшний день нет эффективных способов избежать появления таких ошибок.

Во-вторых, развитие технологий приводит к появлению новых способов проведения атак, и только через некоторое время после их возникновения появляются эффективные способы противодействия им. То есть всегда есть риск того, что в момент проведения атаки защищающаяся сторона окажется неспособна ей противодействовать из-за отсутствия необходимых знаний, опыта или технических средств.

В-третьих, в каждой отдельной организации инциденты, связанные с хакерскими атаками, случаются крайне редко. В то же время для эффективного реагирования на такие атаки требуются люди с крайне редкими специальностями: вирусные аналитики, компьютерные криминалисты и т. п. Ни одна организация не может позволить себе держать в штате таких специалистов, если они востребованы только один-два раза в год. Такая особенность предметной области диктует свой подход к решению проблемы. Если применяемые меры защиты не могут гарантированно предотвратить атаку, значит, одновременно с принятием превентивных мер необходимо готовиться к реагированию на такую атаку. Если невозможно обеспечить все предприятия, входящие в *критическую информационную инфраструктуру*, специалистами с нужными компетенциями,

значит необходимо создавать центры компетенции, которые будут непосредственно подключаться к противодействию атакам. Этот подход и был заложен в концепцию построения государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

ГосСОПКА создана для обмена информацией о кибератаках на информационные системы, нарушение или прекращение работы которых крайне негативно скажется на экономике страны или безопасности граждан.

Деятельность ГосСОПКА регулируют несколько документов:

– Доктрина информационной безопасности Российской Федерации;

– федеральные законы «О безопасности критической информационной инфраструктуры» и «Об информации, информационных технологиях и о защите информации»;

– Стратегия развития информационного общества;

– указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ГосСОПКА);

– Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации;

– Концепция ГосСОПКА;

– Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА.

Список постоянно пополняется, изменяются сами документы из этого списка, поэтому необходимо постоянно отслеживать изменения и приводить свои информационные системы в соответствие текущим требованиям.

Структура системы построена по территориально-ведомственному принципу (рис. 3.1).

Центр ГосСОПКА — совокупность сил и средств субъекта ГосСОПКА, предназначенная для решения задач ГосСОПКА в своей зоне ответственности.

Главный центр (Национальный координационный центр по компьютерным инцидентам-НКЦКИ) — наивысшая структура в иерархии, разрабатывает нормативные документы и методики. За работу этого центра отвечает ФСБ России.

Головной центр — наивысшая структура в иерархии центров, объединённых по ведомственному или организационному признакам.

Подчинённый центр — центр, который структурно подчиняется головному центру.

Сегмент ГосСОПКА — совокупность головного центра и иерархически подчинённых центров.

Ведомственные центры — органы государственной власти.

Корпоративные центры — коммерческие и некоммерческие организации. Могут оказывать услуги подключения к ГосСОПКА при наличии лицензии.

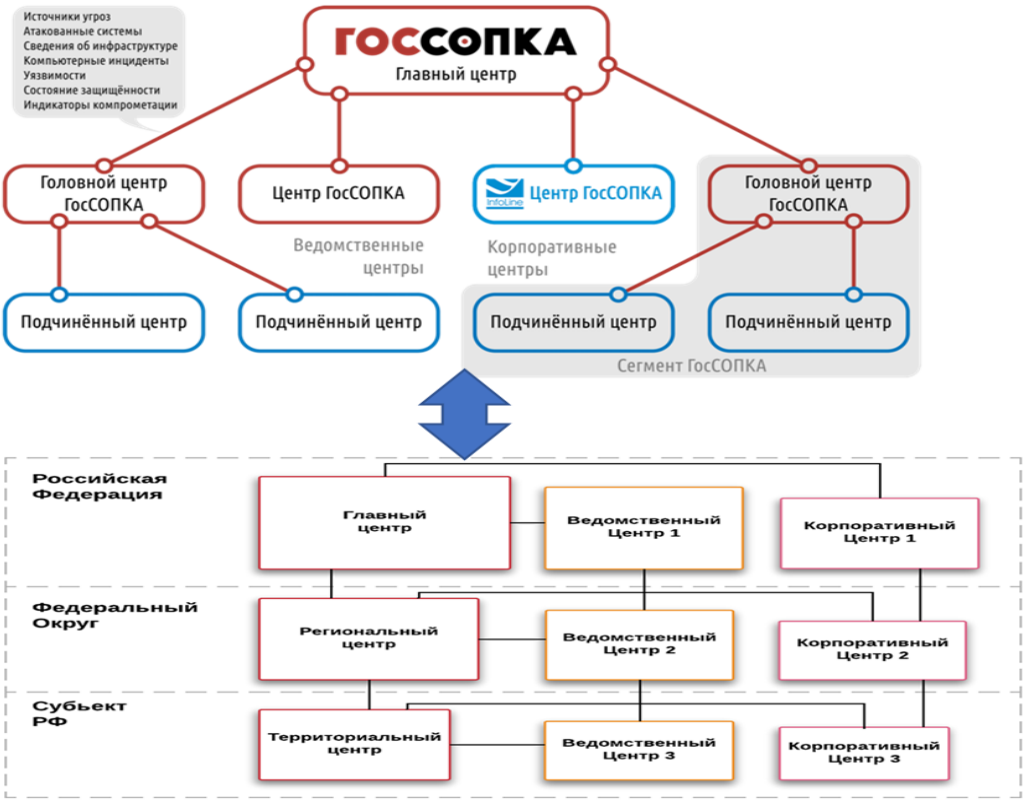


*Рис. 3.1. Структура ГосСОПКА*

К ГосСОПКА должны подключаться владельцы объектов критической информационной инфраструктуры (КИИ). К ним относятся организации здравоохранения, науки, транспорта, связи, энергетики, банковской сферы (системно значимые кредитные организации, операторы платёжных систем, системно значимые инфраструктурные организации финансового рынка), топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

После подключения они обязаны самостоятельно отправлять в систему ГосСОПКА информацию о киберинцидентах, а также о предотвращении и обезвреживании атак на объекты КИИ. Полученная информация аккумулируется и анализируется в НКЦКИ для формирования индикаторов компрометации и бюллетеней информационной безопасности, которые затем адресно рассылаются участникам ГосСОПКА. Это помогает организациям быть в курсе актуальных киберугроз (рис. 3.2).

Кроме сбора сведений об угрозах и информирования участников об идущих атаках, участники ГосСОПКА могут запрашивать содействие со стороны НКЦКИ в реагировании на компьютерные инциденты. Это позволяет им иметь самую актуальную информацию об инцидентах информационной безопасности и способах противодействия им, а как следствие — лучше организовать систему киберзащиты и реагировать на инциденты информационной безопасности быстрее и эффективнее.

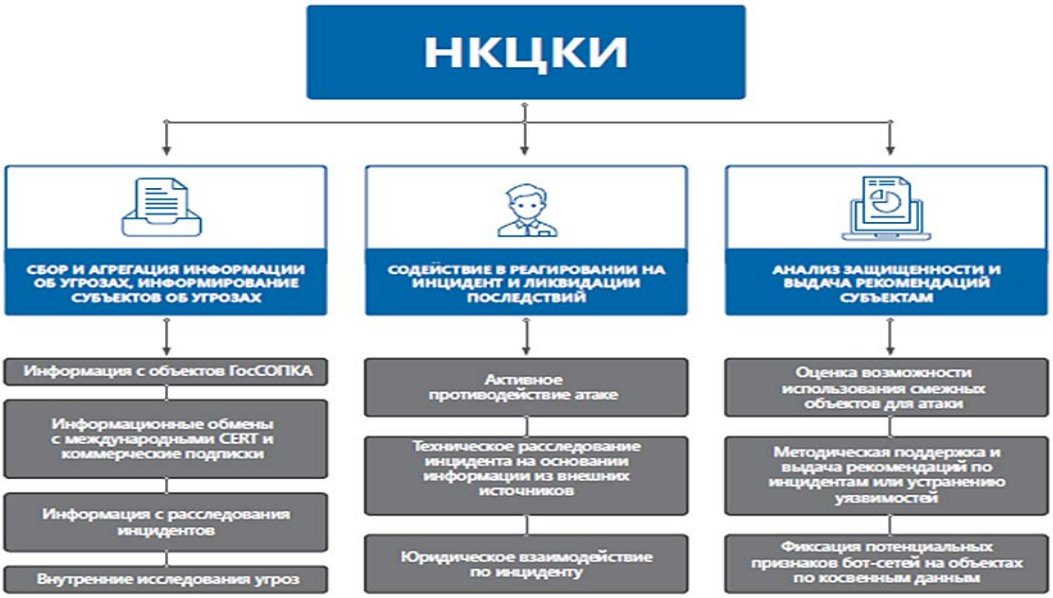


*Рис. 3.2 Структура и схема функционирования НКЦКИ*

Глобально в рамках информационного взаимодействия субъектом КИИ решается несколько критичных для обеспечения функций ГосСОПКА задач:

– определение и поддержание в актуальном состоянии своей зоны ответственности;

– отчетность в сторону вышестоящего центра ГосСОПКА о выявленных и обработанных инцидентах информационной безопасности;

– получение и обработка уведомлений и запросов вышестоящего центра ГосСОПКА.

Рассмотрим эти задачи, оценив значимость обрабатываемой информации и возможное ее использование как для задач НКЦКИ, так и для обеспечения безопасности всей структуры КИИ РФ.

1. В рамках поддержания актуальной информации о зоне ответственности в первую очередь необходим сбор данных об инфраструктуре объекта, в том числе:

– описание внешнего периметра организации и способов выхода в интернет;

– наличие информационных и технологических «стыков» с другими объектами КИИ или прочими информационными системами;

– состояние установленных обновлений и патчей и возможные сроки установки корректирующих патчей;

– структура внутренних сотрудников и внешних подрядчиков, несущих ответственность за функционирование конкретных комплексов.

С точки зрения конкретной организации данная инвентаризационная информация, казалось бы, не имеет существенного отношения к обеспечению информационной безопасности. Но она может совершенно по-другому интерпретироваться на уровне НКЦКИ: при возникновении очередной массовой угрозы или уязвимости появляется возможность корректно оценить, какие именно объекты в состоянии самостоятельно и в штатном режиме устранить уязвимости,

а в каких случаях необходимо более детальное информирование и особый порядок сопровождения конкретной задачи. Ни для кого не секрет, что получение официального письма по задачам информационной безопасности и закрытию уязвимостей из вышестоящих ведомств и органов зачастую позволяет более эффективно построить взаимодействие в компании и дает дополнительные рычаги подразделению информационной безопасности для отстаивания своих позиций.

Информация о «стыках» и подрядчиках приобретает критическое значение, если объект КИИ из смежной организации находится под атакой или в стадии разбора конкретного инцидента.

В этом случае успешная атака на один из объектов или инфраструктуру подрядчика через, как правило, слабо защищаемые информационные стыки может иметь последствия в инфраструктуре другого объекта. Заранее увидеть и предсказать такую ситуацию из своей инфраструктуры невозможно, но в рамках данных, доступных НКЦКИ, такие нюансы могут быть оперативно отработаны.

Наконец, в инфраструктурах не до конца защищенных и распределенных организаций могут находиться средства вычислительной техники, являющиеся частью бот-сети. Зачастую злоумышленники используют скомпрометированные вычислительные ресурсы для атаки на другие инфраструктуры: активных сканирований на уязвимости, брут-форсов, DDoS-атак. В таком случае, если атака направлена на один из объектов КИИ, при анализе технических индикаторов НКЦКИ сможет выявить, что часть ботов использовали для атаки адреса одного из прочих объектов, и в режиме «раннего оповещения» проинформирует ответственные службы о затаившейся в их инфраструктуре угрозе.

2. В рамках отчетности по инцидентам происходит информирование вышестоящего центра ГосСОПКА о выявленных в своей инфраструктуре инцидентах со следующими ключевыми характеристиками:

– техническая информация об атаке (адреса, инструменты, методы);
– результаты реагирования и ликвидации последствий;
– необходимость содействия со стороны вышестоящего центра.

Стоит отметить, что содействие оказывается в рамках полномочий НКЦКИ как российского CERT (*computer emergency response team* – компьютерная группа реагирования на чрезвычайные ситуации), способного выполнять самые разные операции:

– оперативное блокирование доменов/адресов, удаление вредоносных ссылок или разделегирование доменов, осуществляющих вредоносные действия;
– на основании предоставленных сведений выполнение более детального сбора информации о злоумышленниках (получение информации о владельцах и способах оплаты доменов, выявление каналов подключения к инфраструктуре, с которой осуществлялась атака, и другие доступные CERT инструменты атрибуции и поиска злоумышленников);
– вовлечение внутренних или внешних ресурсов в процесс анализа и расследования произошедшего инцидента для восстановления всего сценария атаки и выработки мер противодействия;

– перевод возникшего инцидента в юридическую плоскость и возможность уголовного преследования злоумышленников.

Описанные мероприятия могут помочь как противодействовать развивающейся атаке, так и расследовать уже завершившуюся атаку для уголовного наказания киберпреступников.

Стоит отметить, что НКЦКИ, как национальный CERT, имеет возможность и полномочия работать не только на уровне Российской Федерации, но и взаимодействовать с международными CERT, облачными провайдерами и телекомоператорами для оказания помощи в противодействии инциденту и его дальнейшем расследовании. Это делает возможность атрибуции и нахождения злоумышленников, использующих иностранные хостинги и ip-адреса в атаке, более вероятной, чем при взаимодействии с локальными органами и структурами расследования инцидентов.

3. Обработка уведомлений и запросов вышестоящего центра, включающих в себя информацию:

– о противодействии или блокировании потенциальных атак;

– о сборе информации об определенных событиях информационной безопасности.

В рамках рассмотренных направлений деятельности НКЦКИ собирает и агрегирует информацию по большому количеству угроз и инцидентов, зафиксированных на объектах КИИ. Дополнительно к этой информации в своем внутренней базе угроз НКЦКИ может использовать информацию:

– полученную в рамках информационных обменов с международными CERT и центрами противодействия киберугрозам;

– полученную из коммерческих и некоммерческих источников об угрозах;

– полученную в рамках следственных мероприятий по расследованию инцидентов;

– из систем обнаружения компьютерных атак, установленных на разных объектах;

– собственные внутренние исследования угроз;

– обращения граждан по вопросам противодействия киберугрозам.

Таким образом, НКЦКИ выступает в роли огромного информационного хаба и источника знаний о новых и актуальных угрозах безопасности информации, которая носит практический характер защиты от новых угроз и повышения защищенности конкретного объекта и которая может стать востребованной любым из участников информационного обмена в ГосСОПКА.

## 3.2. Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам

С начала 1970-х годов в ведущих странах мира началось широкомасштабное применение технических средств разведки. 1980-е, ознаменовавшись

бурным научно-техническим прогрессом, особенно в военной области, дали новые импульсы в дальнейшем наращивании возможностей технических средств иностранных разведок. До 70 % разведывательной информации добывалось с помощью технических средств.

Сложившаяся обстановка потребовала совершенствования системы мер противодействия иностранным разведкам. Противоборство с техническими разведками зарубежных стран стало задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны.

Структура и основные функции государственной *системы защиты информации* от ее утечки по техническим каналам и организация работ по защите информации определены в Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам[1].

Именно эту систему часто называют как государственной системой защиты информации или государственной системой технической защиты информации.

С момента принятия данного положения произошли изменения в общественно-политической и экономической жизни страны. Изменилась и структура государственной системы защиты информации. Последние изменения были внесены указом Президента РФ от 11 марта 2003 г. № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации».

Положение определяет структуру государственной системы защиты информации в Российской Федерации, ее задачи и функции, основы организации защиты сведений, отнесенных в установленном порядке к государственной или служебной тайне, от иностранных технических разведок и от ее утечки по техническим каналам.

Государственная система защиты информации представляет собой совокупность органов и исполнителей используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. Является составной частью системы обеспечения национальной безопасности Российской Федерации и призвана защищать безопасность государства от внешних и внутренних угроз в информационной сфере.

Организацию деятельности государственной системы технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровне, а также руководство указанной системой осуществляет ФСТЭК России (рис. 3.3).

Государственная система защиты информации включает в себя подсистемы лицензирования деятельности предприятий в области защиты информации,

[1] Утв. постановлением Правительства РФ от 15.09.1993 № 912-51.

сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.


*Рис. 3.3 . Структура государственной системы защиты информации*

Перечисленные выше подсистемы представляют в совокупности деятельность следующих органов:

– ФСТЭК России и ее территориальных органов (региональные управления в субъектах Российской Федерации);

– федеральных органов исполнительной власти, других органов и организаций Российской Федерации, руководящие работники которых входят в состав коллегии ФСТЭК России по должности (Минюст, Минобороны, МЧС, МВД, МИД, Минпромэнерго, Минэкономразвития, Минприроды, ФСО, ФСБ, СВР, ГУСП (Главное управление специальных программ Президента Российской Федерации), РАН, ЦБР (Центральный банк Российской Федерации));

– структурных подразделений по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации;

– предприятий, проводящих работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделений по защите информации;

– научно-исследовательских организаций по проблемам защиты информации;

– организаций-разработчиков средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации;

– предприятий, оказывающих услуги в области защиты информации.

– организаций Федерального агентства по техническому регулированию и метрологии (Росстандарт)[1], выполняющих работы по стандартизации в области защиты информации;

– органов системы лицензирования деятельности в области защиты информации;

– органов системы сертификации средств защиты информации;

– органов системы аттестации объектов защиты по требованиям безопасности информации.

*Одним из ключевых звеньев государственной системы защиты информации является МВД России*, важнейшей задачей которого является предупреждение, выявление, пресечение, раскрытие и расследование преступлений, в том числе и сопряженных с использованием средств – носителей новых информационных технологий. В этих целях МВД России формирует, ведет и использует федеральные учеты, банки данных и оперативно-справочной, розыскной, криминалистической, статистической и иной информации. Как правило, эта информация носит конфиденциальный характер и является объектом защиты, поскольку утечка подобного рода информации способна не только существенно затруднить деятельность органов внутреннихдел по борьбе с преступностью, но и представляет собой непосредственную угрозу жизни и здоровью сотрудников полиции, лиц, сотрудничающих с правоохранительными органами и оказывающих содействие уголовному судопроизводству.

*Функционирование государственной системы защиты информации осуществляется на основании:*

– Конституции Российской Федерации;

– федеральных законов от 21 июля 1993 г. № 5485-1 «О государственной тайне», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 28 декабря 2010 г. № 390-ФЗ «О безопасности», от 05 июня 1996 г. № 85-ФЗ «Об участии в международном информационном обмене»;

– указов Президента РФ от 11 марта 2003 г. № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации», от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;

– Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим каналам[2];

– Доктрины информационной безопасности Российской Федерации;

– других правовых актов федеральных органов власти в области защиты информации.

Деятельность государственной системы защиты информации реализуется на основе подчиненности Президенту РФ, основываясь на разграничении полномочий федеральных органов исполнительной власти, органов исполнитель-

[1] Бывший Госстандарт России.

[2] Утв. постановлением Совета Министров – Правительства РФ от 15.09.1993 № 912–51.

ной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций по защите информации.

Обеспечение условий, способствующих реализации политики Российской Федерации в сфере безопасности государства, содействие экономическому и научно-техническому прогрессу страны, предотвращение или существенное снижение ущерба национальной безопасности Российской Федерации с использованием методов и средств защиты информации — все это *цели*, преследуемые государственной системой защиты информации.

*Основные задачи* государственной системы защиты информации:

– проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

– исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных специальных программно-технических воздействий на информацию в целях ее разрушения, уничтожения, искажения или блокирования в процессе обработки, передачи и хранения;

– принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;

– общая организация сил, создание средств защиты информации и средств контроля эффективности ее защиты;

– контроль за проведением работ по защите информации в органах государственного управления, объединениях, на предприятиях, в организациях и учреждениях (независимо от форм собственности).

*Главными направлениями работы* по защите информации являются:

– обеспечение эффективного управления системой защиты информации;

– определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;

– анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

– разработка организационно-технических мероприятий по защите информации и их реализация;

– организация и проведение контроля состояния защиты информации.

*Защита информации осуществляется путем выполнения комплекса мероприятий* по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий в целях разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противо-

действию иностранным техническим разведкам, а также путем проведения специальных работ.

Мероприятия по защите информации, обрабатываемой техническими средствами, являются составной частью управленческой, научной и производственной деятельности учреждений и предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению комплекса мер по защите сведений, составляющих государственную и служебную тайну.

В то же время эти мероприятия являются составной частью работ по созданию и эксплуатации систем информатизации учреждений и предприятий, располагающих такой информацией, и должны осуществляться в установленном нормативными документами порядке в виде системы защиты секретной информации.

*Основными организационно-техническими мероприятиями* по защите информации являются:

– лицензирование деятельности предприятий в области защиты информации;

– аттестование объектов по выполнению требований по обеспечению защиты информации при проведении работ со сведениями соответствующей степени секретности;

– сертификация средств защиты информации и контроля за её эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

– категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

– обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;

– оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории Российской Федерации;

– введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

– создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

– разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;

– разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;

– применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случае ее утечки, разрушения (уничтожения). Проведение любых мероприятий и работ с использованием сведений, отнесенных к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается:

1) сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности;

2) по результатам сертификационных испытаний;

3) предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

Контроль состояния защиты информации (далее именуется – контроль) осуществляется в целях своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки защиты ее от иностранных технических разведок.

*Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.* Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

Нарушения по степени важности делятся на три категории:

– невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;

– невыполнение требований по защите информации, в результате чего создаются предпосылки к её утечки по техническим каналам;

– невыполнение других требований по защите информации.

*При обнаружении нарушений первой категории руководители органов государственной власти и предприятий обязаны:*

1) немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;

2) организовать в установленном порядке расследование причин и условий появления нарушений в целях недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

3) сообщить во ФСТЭК, руководству органа государственной власти, федеральному органу государственной безопасности и заказчику о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер, проводимой ФСТЭК или по ее поручению подразделениями по защите информации органов государственной власти.

При обнаружении нарушений второй и третьей категорий руководители проверяемых органов государственной власти и предприятий обязаны принять необходимые меры по их устранению в сроки, согласованные с органом, проводившим проверку, или заказчиком (представителем заказчика). Контроль за устранением этих нарушений осуществляется подразделениями по защите информации этих органов государственной власти и предприятий.

Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесенные к государственной или служебной тайне, проводится аттестование указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

## 3.3. Обеспечение лицензирования, сертификации и аттестации в области защиты информации

Система обеспечения информационной безопасности базируется на своде законов и нормативно правовых документов РФ по лицензированию деятельности в сфере защиты информации, сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

В соответствии с требованиями нормативно-правовой базы Российской Федерации для осуществления деятельности, связанной с использованием государственной тайны и сведений конфиденциального характера, юридическому лицу необходимо иметь соответствующие лицензии и сертификаты.

Законодательство Российской Федерации предусматривает установление Правительством Российской Федерации порядка ведения лицензионной деятельности, перечня видов деятельности, на осуществление которых требуется лицензия, и органов, уполномоченных на ведение лицензионной деятельности.

В соответствии со ст. 12 федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» обязательному лицензированию подлежат следующие виды деятельности (в области защиты информации):

– разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств;

– выполнение работ, оказание услуг в области шифрования информации;

– техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств;

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– разработка и производство средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации.

В рамках рассматриваемых видов деятельности были выпущены отдельные постановления Правительства Российской Федерации, разъясняющие порядок лицензирования. Среди них:

– от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности»;

– от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

– от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

– от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю (ФСТЭК).

*Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:*

– наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;

– наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему по праву собственности или на ином законном основании;

– наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;

– использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и(или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

– использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;

– наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответ-

ствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю.

Таким образом, вся деятельность по обеспечению технической защиты конфиденциальной информации подпадает под обязательное лицензирование, т. е. владелец автоматизированной (информационной) системы, в рамках которой обрабатывается, хранится или передаётся конфиденциальная информация, должен обладать лицензией на проведение работ по технической защите информации либо привлекать для проведения подобных работ компании, обладающие такой лицензией.

Другим важным документом, требующим особого внимания, является постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами». Настоящим постановлением утверждены сразу четыре положения:

– Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств;

– Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств;

– Положение о лицензировании предоставления услуг в области шифрования информации;

– Положение о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Лицензирование по указанным видам деятельности осуществляется Федеральной службой безопасности Российской Федерации.

Лицензирование деятельности в области защиты информации представляет собой определенную форму государственного контроля и должно обеспечить не только допуск организаций, соответствующих определенным требованиям и условиям, к осуществлению определенных видов деятельности, но и повышение качества непосредственно мероприятий и услуг по технической защите информации.

Если говорить о *сертификации применительно к средствам защиты информации,* то это деятельность по подтверждению их соответствия требованиям технических регламентов, национальных стандартов или иных нормативных документов по защите информации.

Саму систему сертификации представляет ФСТЭК России, которому подведомственны аккредитованные органы по сертификации средств защиты информации и испытательные лаборатории.

Нормативная правовая база системы сертификации средств защиты информации включает в себя:

– федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;

– постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;

– Положение о сертификации средств защиты информации по требованиям безопасности информации[1];

– Положение о системе сертификации средств защиты информации[2].

Сертификации подлежат технические, программные, программно-аппаратные средства защиты информации, средства в которых реализованы СЗИ и средства контроля эффективности защиты информации.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации

*Система сертификации средств защиты информации* представляет собой совокупность участников сертификации, которыми являются:

– федеральный орган по сертификации;

– центральный орган системы сертификации — орган, возглавляющий систему сертификации однородной продукции;

– органы по сертификации средств защиты информации — органы, проводящие сертификацию определенной продукции;

– испытательные лаборатории — лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;

– изготовители — продавцы, исполнители продукции.

Центральные органы системы сертификации, органы по сертификации средств защиты информации и испытательные лаборатории проходят *аккредитацию на право проведения работ по сертификации.* Целью аккредитации является проверка возможности выполнения работ по сертификации средств защиты информации. Аккредитация проводится только при наличии у указанных органов и лабораторий лицензии на соответствующие виды деятельности.

*Федеральный орган по сертификации***:**

– создает системы сертификации;

– осуществляет выбор способа подтверждения соответствия средств защиты информации требованиям нормативных документов;

– устанавливает правила аккредитации центральных органов систем сертификации, органов по сертификации средств защиты информации и испытательных лабораторий;

– определяет центральный орган для каждой системы сертификации;

– выдает сертификаты и лицензии на применение знака соответствия;

– ведет государственный реестр участников сертификации и сертифицированных средств защиты информации;

– осуществляет государственные контроль и надзор за соблюдением участниками сертификации правил сертификации и за сертифицированными средствами защиты информации, а также устанавливает порядок инспекционного контроля;

– рассматривает апелляции по вопросам сертификации;

[1] Утв. приказом Гостехкомиссии России от 27.10.1995 № 199

[2] Утв. приказом ФСТЭК России от 03.04.2018 № 55

– представляет на государственную регистрацию в Комитет Российской Федерации по стандартизации, метрологии и сертификации системы сертификации и знак соответствия;

– устанавливает порядок признания зарубежных сертификатов;

– приостанавливает или отменяет действие выданных сертификатов.

*Центральный орган системы сертификации:*

– организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации;

– ведет учет входящих в систему сертификации органов по сертификации средств защиты информации и испытательных лабораторий, выданных и аннулированных сертификатов и лицензий на применение знака соответствия;

– обеспечивает участников сертификации информацией о деятельности системы сертификации.

При отсутствии в системе сертификации центрального органа его функции выполняются федеральным органом по сертификации

*Органы по сертификации средств защиты информации:*

– сертифицируют средства защиты информации, выдают сертификаты и лицензии на применение знака соответствия с представлением копий в федеральные органы по сертификации и ведут их учет;

– приостанавливают либо отменяют действие выданных ими сертификатов и лицензий на применение знака соответствия;

– принимают решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации;

– формируют фонд нормативных документов, необходимых для сертификации;

– представляют изготовителям по их требованию необходимую информацию в пределах своей компетенции.

*Испытательные лаборатории* проводят сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации средств защиты информации и изготовителям. Испытательные лаборатории несут ответственность за полноту испытаний средств защиты информации и достоверность их результатов.

*Изготовители:*

– производят (реализуют) средства защиты информации только при наличии сертификата;

– извещают орган по сертификации, проводивший сертификацию, об изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации;

– маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации;

– указывают в сопроводительной технической документации сведения о сертификации и нормативных документах, которым средства защиты информации должны соответствовать, а также обеспечивают доведение её до потребителя;

– применяют сертификат и знак соответствия, руководствуясь законодательством Российской Федерации и правилами, установленными для данной системы сертификации;

– обеспечивают соответствие средств защиты информации требованиям нормативных документов по защите информации;

– обеспечивают беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих сертификацию, и контроль за сертифицированными средствами защиты информации;

– прекращают реализацию средств защиты информации при несоответствии их требованиям нормативных документов или по истечении срока действия сертификата, а также в случае приостановки действия сертификата или его отмены.

*Основными схемами проведения сертификации средств защиты информации* являются:

– единичных образцов средств защиты информации — проведение испытаний этих образцов на соответствие требованиям по защите информации;

– для серийного производства средств защиты информации — проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований.

В отдельных случаях по согласованию с органом по сертификации средств защиты информации допускается проведение испытаний на испытательной базе изготовителя. Сроки проведения испытаний устанавливаются договором между изготовителем и испытательной лабораторией.

При несоответствии результатов испытаний требованиям нормативных и методических документов по защите информации орган по сертификации средств защиты информации принимает решение об отказе в выдаче сертификата и направляет изготовителю мотивированное заключение.

В случае несогласия с отказом в выдаче сертификата изготовитель имеет право обратиться в центральный орган системы сертификации, федеральный орган по сертификации или в Межведомственную комиссию для дополнительного рассмотрения полученных при испытаниях результатов.

*Аттестация по требованиям безопасности информации* предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

*Аттестация объекта* — официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов по защите информации.

Под аттестацией объекта информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативных документов по защите информации, утвержденных ФСТЭК (Гостехкомиссией) России.

Объектами аттестации являются защищаемые помещения и объекты информатизации в состав которых входят средства и системы непосредственно обрабатывающие защищаемую информацию. В целом, объект аттестации представляет собой совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Аттестацию объектов информатизации могут проводить организации имеющие лицензию на право оказания услуг по технической защите конфиденциальной информации, органы по аттестации объектов информатизации, аккредитованные ФСТЭК России.

*Обязательной аттестации подлежат:*

– объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну;

– объекты информатизации, предназначенные для управления экологически опасными объектами;

– объекты, предназначенные для ведения секретных переговоров;

– объекты, предназначенные для обработки и обсуждения конфиденциальной информации.

В остальных случаях аттестация носит добровольный характер и может осуществляться по желанию заказчика или владельца объекта информатизации при наличии юридически закрепленного его согласия выполнять требования Положения по аттестации объектов информатизации по требованиям безопасности информации.

Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

В нормативную и методическую документацию включаются только те показатели, характеристики и требования, которые могут быть объективно проверены.

В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

Аттестация объектов информатизации проводится в соответствии со следующими нормативными документами:

– Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Гостехкомиссии России 25.11.1994);

– Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утв. приказом Гостехкомиссии России от 05.01.1996 № 3);

– Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (утв. председателем Гостехкомиссии России 25.11.1994);

– Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. РД Гостехкомиссии России (утв. решением Гостехкомиссии России от 30.03.1992);

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утв. приказом Гостехкомиссии России от 30.08.2002 № 282);

– Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России (1998).

– Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам. (утв. первым заместителем председателя Гостехкомиссии России 08.11.2001)

*Разрешительные документы, необходимые для проведения работ по аттестации объектов информатизации:*

– лицензия ФСБ России на осуществление работ с использованием сведений, составляющих государственную тайну;

– лицензия ФСБ России на проведение работ по выявлению электронных устройств перехвата информации (специальная проверка ТСС);

– лицензии ФСТЭК России:

на оказание услуг в области защиты государственной тайны в части ТЗИ (СИ ПЭМИН, аттестация ОИ);

на проведение работ, связанных с созданием СЗИ (установка, монтаж, испытания) (проведение специальных исследований ТСС; установка, настройка и проверка эффективности средств защиты; аттестационные испытания);

– аттестат аккредитации органа по аттестации ФСТЭК России (выдача аттестата соответствия).

*Порядок проведения аттестации объектов информатизации требованиям безопасности информации включает следующие действия:*

– подачу и рассмотрение заявки на аттестацию;

– предварительное ознакомление с аттестуемым объектом;

– испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

– разработку программы и методики аттестационных испытаний;

– заключение договоров на аттестацию;

– проведение аттестационных испытаний объекта информатизации;

– оформление, регистрацию и выдачу «Аттестата соответствия»;

– осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

– рассмотрение апелляций.

Программа аттестационных испытаний согласовывается с заявителем.

«Аттестат соответствия» на объект информатизации, отвечающий требованиям по безопасности информации, оформляется и выдается органом по аттестации по установленной форме заявителю после утверждения заключения по результатам аттестации. Регистрация аттестатов соответствия осуществляется по отраслевому или территориальному признакам органами по аттестации с целью ведения информационной базы аттестованных объектов информатизации и планирования мероприятий по контролю и надзору.

Ведение сводных информационных баз аттестованных объектов информатизации осуществляется федеральным органом по сертификации и аттестации или по его поручению одним из органов надзора за аттестацией и эксплуатацией аттестованных объектов.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки информации и требований по безопасности информации.

При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче «Аттестата соответствия». При этом может быть предложен срок повторной аттестации при условии устранения недостатков.

При наличии непринципиального характера «Аттестат соответствия» может быть выдан после проверки устранения этих замечаний.

В случае изменения условий и технологии обработки защищаемой информации:

– владелец аттестованного объекта обязан известить об этом орган по аттестации;

– орган по аттестации принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

Организационную структуру системы аттестации объектов информатизации образуют:

– федеральный орган по сертификации средств и аттестации объектов информатизации по требованиям безопасности информации;

– органы по аттестации объектов информатизации по требованиям безопасности информации;

– испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;

– заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

*Государственный контроль и надзор, инспекционный контроль за проведением аттестации объектов информатизации* проводится федеральным органом по сертификации и аттестации как в процессе, так и по завершении аттестации, а за эксплуатацией аттестованных объектов информатизации — периодически в соответствии с планом работы по контролю и надзору.

Федеральный орган по сертификации и аттестации может передавать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации аккредитованным органом по аттестации.

Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации объектов информатизации.

Государственный контроль и надзор за соблюдением правил аттестации включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации.

Решение о приостановлении или аннулировании действия «Аттестата соответствия» принимается в случае, когда в результате оперативного принятия организационно — технических мер не может быть восстановлен требуемый уровень безопасности информации.

## 3.4. Нормативно-правовое обеспечение мероприятий технической защиты информации

*Под нормативным обеспечением* будем понимать совокупность законодательных актов, нормативных правовых документов, положений, инструкций, требования которых являются обязательными в рамках деятельности организации (предприятия) при решении вопросов защиты информации.

Нормативно-методическое обеспечение системы защиты информации представляет собой комплекс положений законодательных актов, нормативов, методик, правил, регламентирующих создание и функционирование системы защиты информации, взаимодействие подразделений и лиц, входящих в структуру системы, а также статус органов, обеспечивающих функционирование системы защиты информации.

К содержанию нормативно-методических документов по защите информации предъявляются определенные требования. Информационная система должна быть защищена путем внедрения продуманных правил безопасности. Система защиты информации должна использовать набор правил для того, чтобы определить, может ли данный субъект получить доступ к данному объекту. Для предприятия целесообразно внедрение правил обеспечения безопасности и получение полномочий, с помощью которых можно было бы эффективно реализовать

доступ к конфиденциальной информации. Пользователи, не обладающие соответствующими полномочиями, не должны получать доступ к конфиденциальной информации. Кроме того, необходимо применение дискриминационных методов управления, обеспечивающих доступ к данным только для некоторых пользователей или пользовательских групп, например, исходя из служебных обязанностей. Информационная система должна быть защищена с помощью правил безопасности, которые ограничивают доступ к объектам (файлы, приложения) со стороны субъектов (пользователи).

Нормативные документы, определяющие порядок защиты, должны удовлетворять следующим требованиям:

– соответствовать структуре, целям и задачам предприятия;

– описывать общую программу обеспечения безопасности, включая вопросы эксплуатации и усовершенствования;

– перечислять возможные угрозы информации и каналы ее утечки, результаты оценки опасностей и рекомендуемые защитные меры;

– определять ответственных за внедрение и эксплуатацию всех средств защиты;

– определять права и обязанности пользователей, причем таким способом, чтобы этот документ можно было использовать в суде при нарушении правил безопасности.

В результате нормативное обеспечение организации (предприятия) и их информационных систем и технологий формирует основу применения способов и средств защиты информации, способствующих решению большинства задач защиты информации.

Это объясняется тем, что данный вид обеспечения:

– связывает воедино комплекс организационных мероприятий с техническими процедурами защиты информации;

– обеспечивает единый подход ко всем составляющим процесса обеспечения защиты информации;

– наполняет абстрактную модель защиты информации конкретными организационными, техническими, режимными и иными мероприятиями по защите информации;

– определяет функциональные обязанности подразделений организации (предприятия) и отдельных сотрудников по защите информации;

– создает базу для расследования инцидентов, связанных с нарушением режима защиты информации;

– определяет ответственность сотрудников организации (предприятия) за нарушения в области безопасности информации;

– определяет категории информации, правила её защиты информации, а также правила использования средств защиты информации.

Целями нормативного обеспечения безопасности информации внутри организации (предприятия) являются:

– урегулирование отношений в области обеспечения безопасности информации между подразделениями организации (предприятия);

– устранение отдельных противоречий и пробелов в нормативных актах государства;

– конкретизация норм, устанавливающих ответственность за правонарушения в области обеспечения безопасности информации;

– разграничение полномочий в области обеспечения безопасности информации между руководящими структурами организации (предприятия).

Прежде чем приступить к разработке документов, определяющих порядок защиты информации, нужно провести оценку угроз, определить информационные ресурсы, которые целесообразно защищать в первую очередь, что необходимо для обеспечения их безопасности. Правила должны основываться на здравом смысле. Целесообразно обратить внимание на следующие вопросы:

– принадлежность информации (об информации обязан заботиться тот, кому она принадлежит);

– определение важности информации (пока не определена значимость информации, не следует ожидать проявлений должного отношения к ней).

Если право на сохранение тайны будет признано в вашей организации, то может ли она выработать такие правила, которые обеспечивали бы права пользователей на защиту информации?

Состав нормативно-методического обеспечения может быть определен следующим образом: законодательная база, руководящие методические документы и информационно-справочная база. К первому компоненту относятся: законы, указы президента, постановления правительства, кодексы (гражданский, уголовный, административный), ГОСТы. Во второй компонент могут входить документы министерств и ведомств (ФСТЭК, ФСБ, ФСО, Роскомнадзор и др.), а также документы, разработанные на предприятиях по вопросам защиты информации. В состав информационно-справочной базы входят словари, каталоги, специализированные журналы, справочники, электронные базы данных.

Нормативно-методическая документация должна содержать следующие вопросы защиты информации:

– какие информационные ресурсы защищаются;

– какие программы можно использовать на служебных компьютерах;

– что происходит при обнаружении нелегальных программ или данных;

– дисциплинарные взыскания и общие указания о проведении служебных расследований;

– на кого распространяются правила;

– кто разрабатывает общие указания;

– точное описание полномочий и привилегий должностных лиц;

– кто может предоставлять полномочия и привилегии;

– порядок предоставления и лишения привилегий в области безопасности;

– полнота и порядок отчетности о нарушениях безопасности и преступной деятельности;

– особые обязанности руководства и служащих по обеспечению безопасности;

– объяснение важности правил (пользователи, осознающие необходимость соблюдения правил, точнее их выполняют);

– дата ввода в действие и даты пересмотра;

– кто и каким образом ввел в действие эти правила.

Анализ федеральных нормативных документов показывает, что:

во-первых, эти документы носят концептуальный и (или) рамочный характер;

во-вторых, большое внимание уделяется защите интересов государства в процессе обеспечения безопасности информационной, при взаимодействии с организациями, ведущими деятельность по защите информации и т. д.

Кроме того, эти документы определяют порядок разработки, использования и распространения средств защиты информации, устанавливают уровень ответственности лиц и организаций за нарушение законодательства, определяют права лиц и организаций в отношении государства при проведении работ по обеспечению информационной безопасности.

В то же время для организаций (предприятий), ведущих деятельность по защите информации, в первую очередь интересны следующие вопросы:

– регулирование защиты информации и информационных систем от несанкционированного доступа, использования, раскрытия, распространения, модификации или уничтожения;

– порядок обеспечения целостности, означающей защиту информации от неправомерного изменения или уничтожения, включая гарантии ее подлинности;

– правила обеспечения конфиденциальности, означающей поддержание установленных ограничений доступа и распространения информации, включая закрытость данных о частной жизни и о собственности.

Таким образом, общефедеральный уровень законодательства, устанавливая общие положения по обеспечению информационной безопасности, не конкретизирует нормативные вопросы практической деятельности организаций (предприятий) по защите информации. Эти вопросы раскрываются на уровне общегосударственных программ.

Существующая в стране система нормативно-технической документации, которая обеспечивает решение задач информационной защиты, включает государственные и негосударственные стандарты, руководящие документы ФСТЭК России (Гостехкомиссии), отраслевые стандарты.

В целях совершенствования отечественной нормативной базы ФСТЭК совместно с другими заинтересованными министерствами и ведомствами реализуют новые инициативы в этом направлении. В частности, утверждены государственные стандарты, определяющие критерии оценки безопасности информационных технологий, которые устанавливают требования к формированию заданий по оценке безопасности в соответствии с положениями международных стандартов. По линии ФСТЭК создано несколько руководящих документов, в том числе «Руководство по разработке профилей защиты», «Руководство по регистрации профилей защиты», «Методология оценки безопасности информационных технологий» и «Автоматизированный комплекс разработки профилей защиты».

Перечисленные документы, по сути, представляют собой прямую трансляцию положений международных стандартов ISO на российскую нормативно-техническую базу. В дополнение к ним создаются спецификации на защитные профили для операционных систем, межсетевых экранов, систем управления базами данных, автоматизированных систем учета и т. д.

Государственные стандарты обеспечивают единый подход к обеспечению информационной безопасности и создают хорошую базу для разработки документов по защите информации. Сами же стандарты нормативными документами прямого действия для обеспечения процесса информационной безопасности служить не могут.

Нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

В связи с этим нормативные документы ФСТЭК обладают следующими особенностями:

– регламентируют в основном использование технических средств защиты информации от утечки по побочным каналам;

– не регулируют вопросы, связанные с использованием средств шифрования и электронной подписи;

– направлены на нормативное обеспечение деятельности специальных подразделений по защите информации в государственных организациях;

– устанавливают права и обязанности ФСТЭК;

– регулируют оборот средств технической защиты информации;

– часто имеют характер методических указаний по разработке иных нормативных документов;

– устанавливают режим лицензирования и сертификации.

Новое поколение нормативно-технических документов по безопасности информации ориентировано на применение рисковой модели.

Глобализация информационного пространства требует адаптации отечественной нормативно-правовой базы в области информационной безопасности, путем ее объединения с действующими международными нормами.

Одним из наиболее важных международных документов является международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», часто сокращенно называемый «Общие критерии», определяет инструменты оценки безопасности информационных систем и порядок их использования. Он содержит обобщенный опыт ряда государств по безопасности информационных технологий. В России «Общие критерии» представлены в виде национальных стандартов:

– ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть I. Введение и общая модель;

– ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть 2. Функциональные требования безопасности»;

– ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть 3. Требования доверия к безопасности.

В Общих критериях главное внимание уделяется защите от несанкционированного доступа. В документе проведена классификация набора требований к безопасности информации, определены структуры их группирования и принципы использования, введены оценочные уровни доверия (ОУД).

Требования безопасности, содержащиеся в данном документе, могут уточняться и дополняться по мере совершенствования нормативно-правовой базы, развития информационных технологий и совершенствования методов обеспечения информационной безопасности.

Основной целью Общих критериев является повышение доверия к безопасности продуктов и систем информационных технологий. Положения этого документа направлены на создание продуктов и систем информационных технологий с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политики безопасности с учетом условий применения, что должно обеспечить оптимизацию продуктов и систем информационных технологий по критерию «эффективность – стоимость».

Требования к безопасности конкретных продуктов и систем информационных технологий устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, с учетом условий их применения. При формировании требований должны в максимальной степени использоваться компоненты требований, представленные в стандарте. Допускается использование и других требований безопасности. При этом уровень детализации и способ выражения требований, представленных в стандарте, должны использоваться в качестве образца. Требования безопасности могут задаваться заказчиком в техническом задании на разработку продуктов и систем информационных технологий самостоятельно.

Требования безопасности, являющиеся общими для некоторого типа продуктов и систем информационных технологий, могут оформляться в виде структуры, именуемой «Профиль защиты», определенный как набор требований, состоящий только из компонентов или пакетов функциональных требований и одного из уровней гарантированности. Профиль защиты специфицирует совокупность требований, которые являются необходимыми и достаточными для достижения поставленных целей безопасности.

Результатом оценки безопасности должен быть общий вывод, в котором описана степень соответствия объекта оценки функциональным требованиям и условиям гарантированности.

Помимо Общих критериев в России необходимо дополнительно руководствоваться национальными стандартами:

– ГОСТ 54581-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 1. Обзор и основы;

– ГОСТ 54582-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия;

– ГОСТ 54583-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия.

Компенсировать вопросы стандартизации механизма управления системой защиты информации призвана серия международных стандартов ISO/IEC 27000 в области менеджмента информационной безопасности, которая содержит более 30 документов. В настоящее время в России приняты следующие нормативные документы:

– ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (Данный стандарт выдвигает требования к разработке, внедрению, совершенствованию и сертификации системы управления информационной безопасностью (СУИБ). Он покрывает все типы организаций (коммерческие предприятия, государственные агентства и некоммерческие организации). Стандарт уточняет требования на установку, выполнение, обработку, мониторинг, оценку, поддержание и улучшение документированных функций системы управления информационной безопасностью в контексте процесса управления рисками организации. Также стандарт уточняет требования по установке настроек системы защиты удовлетворяющих индивидуальным требованиям организации или ее частей);

– ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Требования»;

– ГОСТ Р ИСО/МЭК 27011-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО, МЭК 27002;

– ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса;

– ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

Эти стандарты определяют основную базовую функциональность и спецификацию архитектуры системы информационной безопасности и содержат фундаментальные задачи последней. Эти задачи являются отправной точкой

для определения набора принципов формирования политики информационной безопасности.

Вопросы аудита и сертификации изложены в национальном стандарте РФ ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения, а также в ГОСТ Р ИСО/МЭК 27006-2008 Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

Руководство по управлению безопасностью в сфере информационных и телекоммуникационных технологий (модель защиты информационной и телекоммуникационной системы, методику оценки риска и ущерба, требования к администратору по безопасности сети) содержат следующие стандарты:

– ГОСТ Р ИСО/МЭК 13335-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;

– ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;

– ГОСТ Р ИСО/МЭК 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети;

– ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции — первый стандарт из семитомного стандарта серии 27033, который содержит общие требования к построению системы защиты вычислительных сетей.

Требования к построению систем защиты информации от скрытых угроз изложены в следующих документах:

– ГОСТ Р ИСО/МЭК 53113-1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения;

– ГОСТ Р ИСО/МЭК 53113-2-2009Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

Базовый механизм управления инцидентами информационной безопасности содержит ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

Новое поколение стандартов в области защиты информации отличается большей формализацией процесса обеспечения безопасности и более детальным комплексным учетом качественно и количественно проверяемых и управ-

ляемых показателей информационной безопасности. Комплексный учет предполагает комплексный подход к управлению безопасностью, когда на соответствие определенным правилам проверяется не только программно-аппаратная составляющая защиты информации, но и организационно-административные меры по обеспечению информационной безопасности.

## 3.5 Общая характеристика единых систем конструкторской, технологичной и программной документации

Основная цель стандартизации — создание условий, способствующих высокому уровню выпускаемой продукции при резком сокращении трудоемкости монтажно-регулировочных работ и стоимости устройства. Для проведения работ по проектированию, изготовлению, настройке, регулировке, эксплуатации и ремонту разрабатывается техническая (конструкторская и технологическая) документация.

Во всех отраслях промышленности действуют Государственные стандарты, в том числе: ГСС — Государственная система стандартизации; ГСИ — Государственная система, обеспечивающая единство измерений; ЕСКД — Единая система конструкторской документации; ЕСТД — Единая система технологической документации, ЕСПД — единая система программной документации.

*Единая система конструкторской документации (ЕСКД),* ГОСТ 2.001–93 — это комплекс стандартов, устанавливающих взаимосвязанные нормы и правила по разработке, оформлению и обращению конструкторской документации, разрабатываемой и применяемой на всех стадиях жизненного цикла изделий (при проектировании, изготовлении, эксплуатации, ремонте и др.).

Основное назначение стандартов ЕСКД состоит в установлении единых оптимальных правил выполнения, оформления и обращения конструкторской документации, которые обеспечивают:

– применение современных методов и средств при проектировании изделий;

– возможность взаимообмена конструкторской документацией без ее переоформления и с оптимальной комплектностью;

– механизацию и автоматизацию обработки конструкторских документов и содержащейся в них информации;

– высокое качество изделия с учетом его безопасности для жизни и здоровья потребителей и окружающей среды;

– возможность расширения унификации и стандартизации при проектировании изделий;

– упрощение форм конструкторских документов и графических изображений;

– возможность создания единой информационной базы автоматизированных систем (САПР, АСУП и др.).

Установленные стандартами ЕСКД правила и положения по разработке, оформлению и обращению документации распространяются: а) на все виды конструкторских документов; б) на учетно-регистрационную документацию и до-

кументацию на внесение изменений в конструкторские документы; в) на нормативно-техническую и технологическую документацию, а также научно-техническую и учебную литературу в той части, в которой они могут быть для них применены и не регламентируются специальными стандартами и нормативами, например форматы и шрифты для печатных изданий и т. п.

Обозначение стандартов ЕСКД производится по ГОСТ 1.0–92. Номер стандарта составляется из цифры 2, присвоенной классу стандартов ЕСКД, одной цифры (после точки), обозначающей классификационную группу стандартов, двухзначного числа, определяющего порядковый номер стандарта в данной группе, и двух последних цифр (после тире), указывающих две последние цифры года утверждения стандарта.

ГОСТ 2.101–68 устанавливает виды изделий всех отраслей промышленности при выполнении конструкторской документации на детали, сборочные единицы, комплексы, комплекты. Изделия, в зависимости от наличия или отсутствия в них составных частей, делят на не специфицированные (детали) — не имеющие составных частей; на специфицированные (сборочные единицы, комплексы, комплекты) — состоящие из двух и более составных частей.

ГОСТ 2.102–68 устанавливает виды и комплектность конструкторских документов на изделия всех отраслей промышленности.

Чертеж детали — документ, содержащий изображение детали и другие данные, необходимые для ее изготовления и контроля.

Сборочный чертеж — документ, содержащий изображение сборочной единицы и другие данные, необходимые для ее сборки (изготовления) и контроля.

Чертеж общего вида — документ, определяющий конструкцию изделия, взаимодействие его основных составных частей и поясняющий принцип работы изделия.

Теоретический чертеж — документ, определяющий геометрическую форму (обводы) изделий и координаты расположения составных частей.

Габаритный чертеж — документ, содержащий контурное (упрощенное) изображение изделия с габаритными, установочными и присоединительными размерами.

Монтажный чертеж — документ, содержащий контурное (упрощенное) изображение изделия, а также данные, необходимые для его установки (монтажа) на месте применения.

Схема — документ, на котором показаны в виде условных изображений или обозначений составные части изделий и связи между ними.

Спецификация — документ, определяющий состав сборочной единицы, комплекса или комплекта. Ведомость спецификаций — документ, содержащий перечень всех спецификаций составных частей изделия с указанием их количества.

Пояснительная записка — документ, содержащий описание устройства и принципа действия разрабатываемого изделия, а также обоснование принятых при его разработке технических и технико-экономических решений.

Технические условия — документ, содержащий требования (совокупность всех показателей, норм, правил и положений) к изделию, его изготовле-

нию, контролю, приемке и поставке, которые нецелесообразно указывать в других конструкторских документах.

Патентный формуляр — документ, содержащий сведения о патентной чистоте объекта, а также о созданных и использованных при его разработке отечественных изобретениях.

Документы в зависимости от стадии разработки подразделяются на проектные (техническое предложение, эскизный проект и технический проект) и рабочие (рабочая документация).

При определении комплектности конструкторских документов на изделие следует различать: а) основной конструкторский документ для деталей — чертеж детали, для сборочных единиц, комплексов и комплектов — спецификация; б) основной комплект конструкторских документов изделия — конструкторские документы, относящиеся ко всему изделию, например, сборочный чертеж, принципиальная электрическая схема, технические условия, эксплуатационные документы; в) полный комплект конструкторских документов, состоящий из основного комплекта конструкторских документов на данное изделие и основных комплектов конструкторских документов на все составные части данного изделия, применяемых по своим основным конструкторским документам.

По виду элементов, входящих в состав изделия, связей между ними и назначения схемы подразделяют на виды и типы по ГОСТ 2.701–84. *Структурные схемы* определяют основной состав изделия и его функциональные части, их назначение и взаимосвязи. *Функциональные схемы* поясняют процессы, происходящие в отдельных функциональных узлах и частях изделия или в изделии в целом. *Принципиальные схемы* определяют полный состав элементов и связей между ними и дают детальное представление о принципе работы изделия. *Схемы соединений* показывают соединения составных частей изделия и определяют провода, жгуты, кабели и другие соединительные изделия, а также места их присоединения и ввода. *Схемы подключений* показывают внешние подключения изделия. *Общие схемы* определяют составные части комплекса и соединения их между собой на месте эксплуатации. *Схемы расположения* устанавливают взаимное расположение отдельных составных частей комплекса, а при его необходимости и соединяющих их жгутов, проводов, кабелей.

*На схеме электрической структурной* (Э1) показывают все функциональные части ЭВМ и основные взаимосвязи между ними. *На схеме электрической функциональной (Э2)* показывают функциональные части устройства, участвующие в процессе, иллюстрируемом схемой, и связи между этими частями. *На схеме электрической принципиальной (Э3)* указывают все элементы, необходимые для построения ЭВМ, связи между элементами и элементы, которые заканчивают входные и выходные цепи. *На схеме электрической соединений (Э4)* изображают либо внешние соединения устройств, входящих в состав ВТ, либо соединения между элементами внутри устройств и блоков устройства.

Состав и правила выполнения технологической документации определяется ГОСТ 3.1001–81 *Единая система технологической документации (ЕСТД).* Она представляет собой комплекс государственных стандартов и руководящих

нормативных документов, устанавливающих взаимосвязанные правила и положения по порядку разработки, комплектации, оформления и обращения технологической документации, применяемой при изготовлении и ремонте изделий (контроль, испытания и перемещения).

Основное назначение ЕСТД — в установлении во всех организациях и на всех предприятиях единых правил выполнения, оформления, комплектации и обращения технологической документации в зависимости от типа и характера производства. Состав документов зависит от стадии разработки ТП, типа и характера производства.

В условиях серийного и массового производства используются документы (ГОСТ 3.1102–81): карта эскизов (КЭ); технологическая инструкция (ТИ); карты маршрутная (МК), технологического процесса (КТП), операционная (ОК), типового (группового) ТП (КТТП), типовой (групповой) операции (КТО), комплектовочная (КК), технико-нормировочная (ТНК), наладки (КН); ведомость технологических маршрутов (ВТМ); ведомость деталей (сборочных единиц) к типовому (групповому) ТП (операции) (ВТП, ВТО).

Наиболее часто используется следующая документация:

– *маршрутная карта* — является обязательным документом, предназначена для маршрутного описания технологического процесса или полного указания состава технологической операции, включая контроль и перемещения по всем операциям в технологической последовательности с указанием данных об оборудовании, технологической оснастке, материальных нормативах и трудовых затратах (допускается взамен МК использовать соответствующую карту ТП);

– *карта ТП* — для операционного описания ТП изготовления или ремонта изделия (составных частей) в технологической последовательности по всем операциям одного вида формообразования, обработки, сборки или ремонта, с указанием переходов, технологических режимов и данных о средствах технологического оснащения, материальных и трудовых затратах;

– *операционная карта* — имеет описание ТО с указанием переходов, режимов обработки и данных о средствах технологического оснащения. Она используется на рабочем месте;

– *карта типового ТП* — для описания типового ТП изготовления или ремонта деталей и сборочных единиц, а *карта типовой ТО* — для описания типовой ТО.

Правила оформления технологических документов приведены в ГОСТ 3.110Ф – 81.

*ЕСПД — единая система программной документации* — комплекс государственных стандартов, устанавливающих взаимосвязанные правила разработки, оформления и обращения программ и программной документации.

В Состав ЕСПД входят:

ГОСТ 19.001 ЕСПД. Общие положения;

ГОСТ 19.004 ЕСПД. Термины и определения;

ГОСТ 19.101 ЕСПД. Виды программ и программных документов;

ГОСТ 19.102 ЕСПД. Стадии разработки;

ГОСТ 19.103 ЕСПД. Обозначения программ и программных документов;

ГОСТ 19.104 ЕСПД. Основные надписи;

ГОСТ 19.105 ЕСПД. Общие требования к программным документам;

ГОСТ 19.106 ЕСПД. Требования к программным документам, выполненным печатным способом;

ГОСТ 19.201 ЕСПД. Техническое задание. Требования к содержанию и оформлению;

ГОСТ 19.202 ЕСПД. Спецификация. Требования к содержанию и оформлению;

ГОСТ 19.401 ЕСПД. Текст программы. Требования к содержанию и оформлению;

ГОСТ 19.402 ЕСПД. Описание программы;

ГОСТ 19.501 ЕСПД. Формуляр. Требования к содержанию и оформлению;

ГОСТ 19.502 ЕСПД. Общее описание. Требования к содержанию и оформлению;

ГОСТ 19.503 ЕСПД. Руководство системного программиста. Требования к содержанию и оформлению;

ГОСТ 19.504 ЕСПД. Руководство программиста. Требования к содержанию и оформлению;

ГОСТ 19.505 ЕСПД. Руководство оператора. Требования к содержанию и оформлению;

ГОСТ 19.506 ЕСПД. Описание языка. Требования к содержанию и оформлению.

ГОСТ 19.601 ЕСПД. Общее правила дублирования, учета и хранения;

ГОСТ 19.602 ЕСПД. Правила дублирования, учета и хранения программных документов, выполненных печатным способом;

ГОСТ 19.603 ЕСПД. Общие правила внесения изменений;

ГОСТ 19.604 ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом;

ГОСТ 19.001 ЕСПД. Общие положения.

В стандартах ЕСПД устанавливают требования, регламентирующие разработку, сопровождение, изготовление и эксплуатацию программ, что обеспечивает возможность:

– унификации программных изделий для взаимного обмена программами и применения ранее разработанных программ в новых разработках;

– снижения трудоемкости и повышения эффективности разработки, сопровождения, изготовления и эксплуатации программных изделий;

– автоматизации изготовления и хранения программной документации.

Правила и положения, устанавливаемые в стандартах ЕСПД распространяются на программную документацию для вычислительных машин, комплексов и систем независимо от их назначения и области применения.

### *Вопросы и задания для самоконтроля*

1. Дайте краткую характеристику государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

2. В чём разница процедур лицензирования, сертификации и аттестации в области защиты информации?

3. Для каких целей используются единые системы конструкторской, технологичной и программной документации?

4. Что входит в состав нормативно-правового обеспечения мероприятий технической защиты информации?

# ЗАКЛЮЧЕНИЕ

Современная информационная среда профессиональной деятельности сотрудника органов внутренних дел — это не простой механизмом, где работают такие компоненты, как электронное оборудование, программное обеспечение, персонал. Это сложная организационно-техническая система, в которой обеспечение информационной безопасности является комплексной проблемой, решение которой предполагает совместное использование законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из средств может привести к потере или утечке информации, цена и роль которой в современном обществе приобретает все более существенное значение.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа — все это выливается в крупные материальные потери, наносит ущерб репутации организации. Способы обеспечения информационной безопасности должны быть ориентированы на упреждающий характер действий, направляемых на заблаговременное принятие мер предупреждения возможных угроз информационной безопасности. Выбор необходимой совокупности способов обеспечения информационной безопасности обусловливается требуемым уровнем защищенности объекта информатизации, масштабностью осуществляемых в отношении его воздействий.

Обеспечение информационной безопасности становится сложнее и актуальнее по мере развития цифрового мира. С практической точки зрения понятие информационной безопасности меняется по мере изменений в мире, некоторые направления защиты информации уходят в прошлое, возникают новые. Задачи усложняются, многие из них лежат в совершенно новых сферах, среди которых:

– разработка кибероружия;

– криптовалюты и токены;

– телемедицина;

– среда виртуализации.

Новые направления защиты информации из кабинетов разработчиков интенсивно переходят в сферу практического применения. Каждый год на рынке появляются новые продукты, позволяющие решить задачи информационной безопасности, что, в свою очередь, требует постоянного повышения уровня профессиональных знаний специалистов по информационной безопасности.

Реалии сегодняшнего дня говорят о том, что миссия обеспечения информационной безопасности трудна, во многих случаях трудновыполнима, но всегда благородна.

Авторы выражают надежду, что материалы учебного пособия «Организационно-правовые основы технической защиты конфиденциальной информации» будут способствовать повышению качества подготовки обучающихся в рамках программы дополнительной профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации».

# СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

*Нормативные правовые акты* [*]

1. Конституция Российской Федерации.
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности.
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
6. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».
8. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

*Литература*

*Основная*

1. Васильева И.Н., Смирнова О.Г. Основы информационной безопасности в ОВД: учебное пособие. – Санкт-Петербург: Изд-во СПб ун-та МВД России, 2017. –124 с.
2. Ищейнов В.Я., Мецатунян М.В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. – Москва: ФОРУМ, 2014. – 256 с.
3. Родин В.Н., Синещук Ю.И., Локнов А.И. [и др.]. Техническая защита информации: учебное пособие. – Санкт-Петербург: Изд-во СПб ун-та МВД России, 2021. – 156 с.
4. Синещук Ю.И., Иванов А.Ю., Родин В.Н. Организационная защита информации: учебное пособие. Часть 1: Методологические основы организационной защиты информации. – Санкт-Петербург: Изд-во СПб ун-та МВД России, 2019. –156 с.
5. Синещук Ю.И., Иванов А.Ю., Родин В.Н. Организационная защита информации: учебное пособие. Часть 2: Прикладные вопросы организационной защиты информации. – Санкт-Петербург: Изд-во СПб ун-та МВД России, 2019. –172 с.

[*] Все нормативные правовые акты приводятся по данным официального интернет-портала правовой информации pravo.gov.ru (дата обращения: 20.01.2023).

6. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. – Москва: Форум, 2018. – 352 с.

*Дополнительная*

1. Грибунов О.П., Старичков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. – Москва: ДГСК МВД Росии, 2017. – 160 с.

2. Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации: учебное пособие. – Москва: НИЯУ МИФИ, 2015. − 152 с.

3. Новиков В.К., Голубчиков С. В. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения: учебное пособие. – 2-е изд. – Москва: Горячая Линия - Телеком, 2019. – 219 с.

4. Синещук Ю.И., Терехин С.Н., Смирнов А.С. [и др.] Безопасность информационных систем и защита информации в МЧС России. учебное пособие.– Санкт-Петербург: СПбУ ГПС МЧС России, 2012. – 256 с.

5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. – Москва: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. – 592 с.

*Электронные ресурсы*

1. http:// anti-malware.ru – информационно-аналитический сайт по информационной безопасности.

2. http://www.fstec.ru – официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

3. securitypolicy.ru – открытая библиотека документов по информационной безопасности.

Учебное издание

*Синещук Юрий Иванович,*
доктор технических наук, профессор
заслуженный работник высшей школы
Российской Федерации;
*Локнов Алексей Игоревич,*
кандидат технических наук;
*Родин Владимир Николаевич,*
кандидат технических наук, доцент;
*Саратов Дмитрий Николаевич,*
кандидат технических наук, доцент

# ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Учебное пособие

Редактор *Свикша Н.О.*
Компьютерная вёрстка *Свикша Н.О.*
Дизайн обложки *Шеряй А.Н.*

ISBN 978-5-91837-677-5

Подписано в печать 13.02.2023. Формат 60×84 $^{1}/_{16}$
Печать цифровая 5,0 п. л. Тираж 100 экз. Заказ № 6/23

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1