# Государственная система защиты информации.

**Учебные вопросы:**

1. Термины и определения в области защиты информации

2. Государственной системы защиты информации.

3. Задачи органов Государственной системы защиты информации.

4. Административная и уголовная ответственность в сфере защиты информации

# Введение

Термин "информационная безопасность" может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры

ГОСТ "Защита информации. Основные термины и определения" вводит понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

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

• **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

• **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

**Угрозы можно классифицировать по нескольким критериям:**

• по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;

• по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

• по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);

• по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход.

*Выделяют следующие уровни защиты информации:*

1. законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;

2. административный – комплекс мер, предпринимаемых локально руководством организации;

3. процедурный уровень – меры безопасности, реализуемые людьми;

4. программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

# Термины и определения в области защиты информации

ФЗ "Об информации, информационных технологиях и о защите информации"

В российском законодательстве базовым законом в области защиты информации является ФЗ **"Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ.** Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

**Закон регулирует отношения, возникающие при:**

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

• применении информационных технологий;

• обеспечении защиты информации.

Закон дает основные определения в области защиты информации.

Приведем некоторые из них:

**• информация** - сведения (сообщения, данные) независимо от формы их представления;

• **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

• **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

• **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

• **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

• **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [4].

**В статье 3 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:**

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2. установление ограничений доступа к информации только федеральными законами;

3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6. достоверность информации и своевременность ее предоставления;

7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся информация делится на общедоступную и ограниченного доступа. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. В законе, определяется информация, к которой нельзя ограничить доступ, например, информация об окружающей среде или деятельности государственных органов. Оговаривается также, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

**Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:**

1. информацию, свободно распространяемую;

2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4. информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

**Дается следующее определение защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:**

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

2. соблюдение конфиденциальности информации ограниченного доступа;

3. реализацию права на доступ к информации.

**Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:**

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

2. своевременное обнаружение фактов несанкционированного доступа к информации;

3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

6. постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ ""Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет права и обязанности его субъектов.

**Следует обратить внимание не определения, приведённые ниже:**

1. ***Защищаемая информация*** - информация, являющаяся предметом  
собственности и подлежащая защите в соответствии с требованиями правовых  
документов или требованиями, устанавливаемыми собственником информации.

*Примечание:*

*Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.*

2. ***Защита информации*** - защита информации: Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

3. ***Защита инфо******рмации от*** ***утечки*** - деятельность по предотвращению  
неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

4. ***Защита инфо******рмации от несанкционированного воздействия*** - защита информации от НСВ: Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

5. ***Зашита инфо******рмации от неп******реднамеренного воздействия*** - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

6. ***Защита информации от разглашения*** - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

7. ***Защита информации от несанкционированного дост******упа*** - защита  
информации от НСД: Деятельность по предотвращению получения защищаемой  
информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

*Примечание:*

*Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.*

8. ***Защита информации от*** ***[иностранной******] разведки*** - деятельность по  
предотвращению получения защищаемой информации [иностранной] разведкой.

9. ***Защита информации от [иностранной] технической разведки*** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой с помощью технических средств.

10. ***Защита информации от агент******урной разведки*** - деятельность по  
предотвращению получения защищаемой информации агентурной разведкой.

11. ***Цель защиты информации*** - желаемый результат защиты информации.

*Примечание:*

*Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.*

12. ***Эффективность защиты информации*** - степень соответствия результатов защиты информации поставленной цели.

13. ***Показатель эффективности зашиты инфо******рмации*** - мера или характеристика для оценки эффективности защиты информации.

14. ***Нормы эффективности защиты информации*** - значения показателей эффективности защиты информации, установленные нормативными документами.

**Организация защиты информации**

15. ***О******рганизация защиты информации*** - содержание и порядок действий  
по обеспечению защиты информации.

16. ***Система защиты информации*** - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

17. ***Мероприятие по защите информации*** - совокупность действий по  
разработке и/или практическому применению способов и средств защиты информации.

18. ***Мероприятие по контролю эффективности защиты информации***- совокупность действий по разработке и/или практическому применению методов  
[способов] и средств контроля эффективности защиты информации.

19. ***Техника защиты информации*** - средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

20. ***Объект защиты*** - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

21. ***Способ защиты информации*** - порядок и правила применения определенных принципов и средств защиты информации.

22. ***Категорирование защищаемой информации*** ***[объекта защиты******]*** - установление градаций важности защиты защищаемой информации [объекта защиты].

23. ***Метод*** ***[способ******] контроля эффективности защиты информации*** - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

24. ***Контроль состояния защиты информации*** - проверка соответствия  
организации и эффективности защиты информации установленным требованиям  
и/или нормам в области защиты информации.

25. ***Средство защиты информации*** - техническое, программное средство,  
вещество и/или материал, предназначенные или используемые для защиты информации.

26. ***Средство контроля эффективности защиты информации*** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

27. ***Контроль организации защиты информации*** - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

28. ***Контроль эффективности защиты информации*** - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

29. ***Организационный контроль эффективности зашиты инфо******рмации***-  
проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

30. ***Технический контроль эффективности зашиты информации*** - контроль эффективности защиты информации, проводимой с использованием средств контроля.

# Основы государственной системы защиты информации.

**“Положение о государственной система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам”** Утверждено постановлением Совета Министров – Правительством Российской Федерации от 15 сентября 1993 г. № 912-51.

Определяет задачи и структуру государственной система защиты информации в Российской Федерации.

Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, во всех органах власти и прочих организациях независимо от их организационно-правовой формы и формы собственности.

**“Положение о государственной система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам”** Утверждено постановлением Совета Министров – Правительством Российской Федерации от 15 сентября 1993 г. № 912-51.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации. Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

**Главные направления работ по защите информации:**

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.

**Основные организационно-технические мероприятиям по защите информации:**

лицензирование деятельности предприятий в области защиты информации;

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

сертификация средств защиты информации и контроля за ее 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 оборонительной, экономической, политической и научно-технической и других сферах деятельности государства;

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

оповещение о пролетах космических и других 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.

**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 программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения;

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

анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;

организация сил, создание средств защиты информации и контроля за ее эффективностью;

контроль состояния защиты информации в органах государственной власти и на предприятиях.

## Организационная структура Государственной системы защиты информации



Целями защиты информации являются:

**Целями защиты информации являются:**

предотвращение утечки информации по техническим каналам;

предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации;

соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;

сохранение возможности управления процессом обработки и пользования информацией.

**Защита информации осуществляется путем:**

предотвращения перехвата техническими средствами информации, передаваемой по каналам связи;

предотвращения утечки обрабатываемой информации за счет ПЭМИН, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;

исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

**Категории нарушений по степени важности**

Первая - невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность её утечки по техническим каналам;

Вторая - невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам;

Третья - невыполнение других требований по защите информации.

## Структура правовой защиты информации



Система документов в области технической защиты информации (ФСТЭК)



Основные подходы государственной политики по   
обеспечению информационной безопасности

# Задачи органов Государственной системы защиты информации.

Ведомственные правовые документы, определяющие права и функции основных элементов ГСЗИ:

“Положение о государственной система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам” Утверждено постановлением Совета Министров – Правительством Российской Федерации от 15 сентября 1993 г. № 912-51.

“Положение о Федеральной службе по техническому и экспортному контролю” Утверждено Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

“Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации” Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 5 января 1996 г. № 3.

“Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации” Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 5 января 1996 г. № 3.

“Типовое положение об испытательной лаборатории” Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 25 ноября 1994 г.

“Положение о Межведомственной комиссии по защите государственной тайны” Утверждено Указом Президента Российской Федерации от 6 октября 2004 г. № 1286



проводят единую техническую политику, осуществляют координацию и методическое руководство работами по защите информации на подведомственных органу государственной власти предприятиях;

выполняют функции заказчика по проведению научно-исследовательских и опытно-конструкторских работ по проблемам защиты информации, а также заказчика поисковых научно-исследовательских работ по этим проблемам;

разрабатывают предложения для федеральных программ по защите информации;

организуют аттестование подведомственных органу государственной власти объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности, сертификацию средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам, проведение специальных проверок и специальных исследований технических средств;

готовят рекомендации и указания по лицензированию деятельности предприятий в области защиты информации.



проверяют и оценивают состояние защиты информации и оказывают методическую помощь на местах в организации и проведении мероприятий по защите информации;

участвуют в аттестовании объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

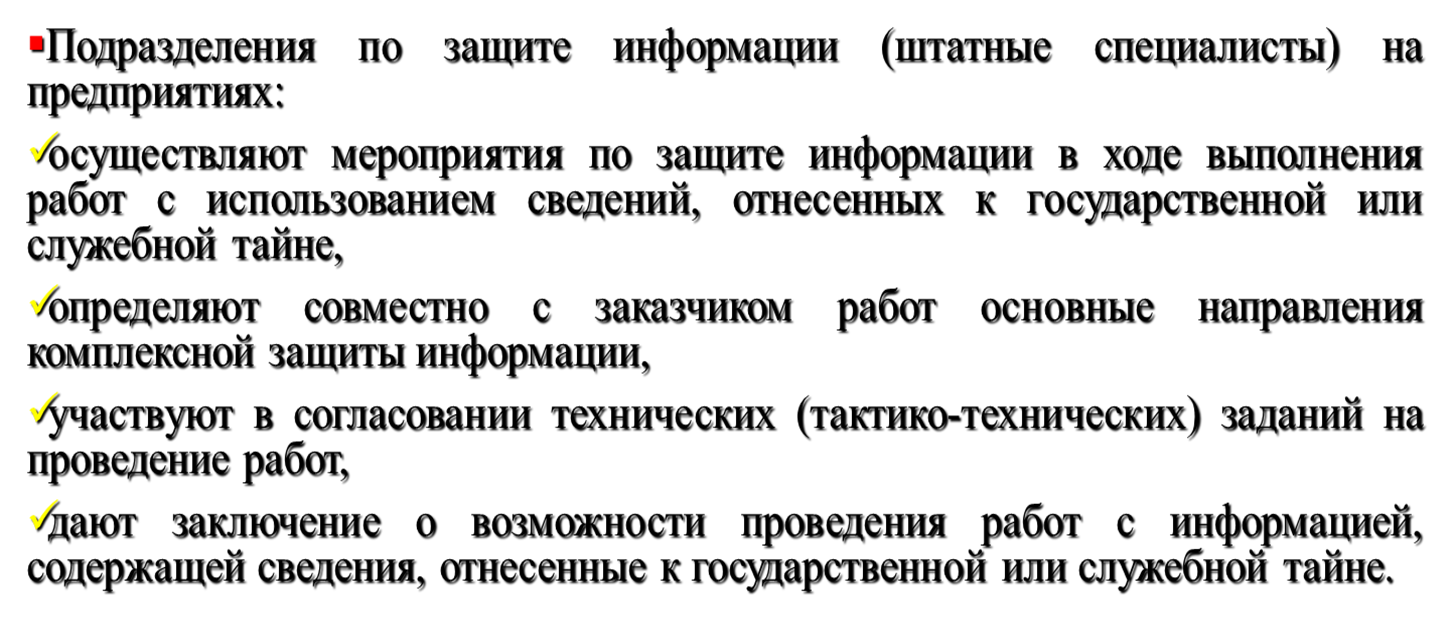
осуществляют активное противодействие возможному ведению разведки техническими средствами их мест постоянного или временного пребывания иностранных граждан на территории Российской Федерации.



* В пределах своей специализации разрабатывают:
* научные основы и концепции,
* проекты федеральных программ,
* нормативно-технических и методических документов по защите информации;
* Обобщают и анализируют информацию о силах и средствах технической разведки, прогнозируют ее возможности;
* Осуществляют разработку (корректировку) модели иностранной технической разведки и методик оценки ее возможностей;
* Проводят научные исследования и работы по созданию технических средств защиты информации и контроля за ее эффективностью.



Организация работ по защите информации на предприятиях осуществляется их руководителями. В зависимости от объема работ по защите информации руководителем предприятия создаются структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.



Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации.





**Осуществляют:**

первичную подготовку специалистов по комплексной защите информации;

переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;

усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

**Организационная структура государственной системы лицензирования деятельности предприятий в области защиты информации**



**Лицензионные центры**



**Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации**



# Административная и уголовная ответственность в сфере защиты информации

Достижения компьютерных технологий за последние годы не только способствовали развитию экономики, торговли и коммуникаций, обеспечили эффективный информационный обмен, но и предоставили уникальный инструментарий лицам, совершающим компьютерные преступления. Чем более интенсивно идет процесс компьютеризации, тем все более реальным становится рост компьютерной преступности, причем современное общество не только ощущает экономические последствия компьютерных преступлений, но и становится все более зависимым от компьютеризации. Она затрагивает многие стороны общественной жизни от контроля за воздушным и наземным транспортом до решения проблем национальной безопасности.

К компьютерным преступлениям относят совершенные с помощью вычислительной техники, традиционные по характеру преступные деяния такие, как кража, мошенничество, подделка и причинение вреда, за которые предусматриваются уголовные санкции в законодательных системах всех стран.

В практической деятельности Российских правоохранительных органов использование автоматизированных информационных систем для совершения любых преступлений оценивается как способ совершения преступления, а используемые программные средства выступают как орудия совершения преступлений. К орудиям и средствам совершения преступления относятся: компьютерная техника, программные средства, магнитные носители.

Существующие нормативно-правовые документы предусматривают административную и уголовную ответственность за нарушения в сфере защиты информации.

Кодекс Российской Федерации об административных правонарушениях  
от 30 декабря 2001 года № 195-ФЗ

**Статья** 13.11. Нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

на граждан в размере от 3 до 5 МРОТ;

для должностных лиц от 5 до 10 МРОТ;

для юридических лиц от 50 до 100 МРОТ.

**Статья** 13.12. Нарушение правил защиты информации.

Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

на граждан в размере от 3 до 5 МРОТ;

на должностных лиц - от 5 до 10 МРОТ;

на юридических лиц - от 50 до 100 МРОТ.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну).

Административный штраф:

на граждан в размере от 5 до 10 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой;

на должностных лиц - от 10 до 20 МРОТ;

на юридических лиц - от 100 до 200 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой.

Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей ГТ, созданием средств, предназначенных для ЗИ, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей ГТ.

Административный штраф:

на должностных лиц в размере от 20 до 30 МРОТ;

на юридических лиц - от 150 до 200 МРОТ.

Использование несертифицированных средств, предназначенных для ЗИ, составляющей ГТ.

Административный штраф:

на должностных лиц в размере от 30 до 40 МРОТ;

на юридических лиц - от 200 до 300 МРОТ с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)

Административный штраф

на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица от 10 до 15 МРОТ или административное приостановление деятельности на срок до девяноста суток;

на должностных лиц - от 10 до 15 МРОТ;

на юридических лиц - от 100 до 150 МРОТ или административное приостановление деятельности на срок до девяноста суток.

Примечание. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

**Статья** 13.13. Незаконная деятельность в области защиты информации.

Занятие видами деятельности в области ЗИ (за исключением информации, составляющей ГТ) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).

Административный штраф:

на граждан в размере от 5 до 10 МРОТ с конфискацией средств защиты информации или без таковой;

на должностных лиц - от 20 до 30 МРОТ с конфискацией средств защиты информации или без таковой;

на юридических лиц - от 100 до 200 МРОТ с конфискацией средств защиты информации или без таковой.

Занятие видами деятельности, связанной с использованием и ЗИ, составляющей ГТ, созданием средств, предназначенных для ЗИ, составляющей ГТ, осуществлением мероприятий и (или) оказанием услуг по ЗИ, составляющей ГТ без лицензии.

Административный штраф:

на должностных лиц в размере от 40 до 50 МРОТ;

на юридических лиц - от 300 до 400 МРОТ с конфискацией созданных без лицензии средств защиты информации, составляющей ГТ, или без таковой.

**Статья** 13.14. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Административный штраф:

на граждан в размере от 5 до 10 МРОТ;

на должностное лицо - от 40 до 50 МРОТ.

Уголовный кодекс Российской Федерации  
от 13 июня 1996 года № 63-ФЗ

**Статья** 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации:

штраф в размере до 200000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев,

либо обязательные работы на срок от 120 до 180 часов,

либо исправительные работы на срок до 1 года,

либо арест на срок до 4 месяцев.

2. Те же деяния, совершенные лицом с использованием своего служебного положения:

штраф в размере от 150000 до 300000 рублей или в размере заработной платы или иного дохода осужденного за период от одного года до 2 лет,

либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет,

либо арест на срок от 4 до 6 месяцев.

**Статья** 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан:

штраф в размере до 80000 рублей, или в размере заработной платы или иного дохода осужденного за период до шести месяцев,

либо обязательные работы на срок от 120 до 180 часов,

либо исправительные работы на срок до 1 года.

2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации:

штраф в размере от 150000 до 300000 рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет,

либо лишение права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет,

либо обязательные работы на срок от ста восьмидесяти до двухсот сорока часов,

либо арест на срок от 2 до 4х месяцев.

3. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации:

штраф в размере до 200000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев,

либо ограничение свободы на срок до 3 лет,

либо лишение свободы на срок до 3 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет

**Статья** 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом:

штраф в размере до 80000 тысяч рублей или в размере заработной платы или иного дохода осужденного за период от 1 до 6 месяцев,

либо лишение свободы на срок до 2 лет.

Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе:

штраф в размере до 120000 рублей или в размере заработной платы или иного дохода осужденного за период до 1 года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо лишение свободы на срок до 3 лет.

Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности:

штраф в размере до 200000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо лишение свободы на срок до 5 лет.

Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия:

лишение свободы на срок до 10 лет.

**Статья** 272. Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

штраф в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев,

либо исправительные работы на срок от 6 месяцев до 1 года,

либо лишение свободы на срок до 2 лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

штраф в размере от 500 до 800 МРОТ, в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев.

исправительные работы на срок от 1 года до 2 лет.

арест на срок от 3 до 6 месяцев.

лишение свободы на срок до 5 лет.

**Статья** 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

лишение свободы на срок до 3 лет со штрафом в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от 2 до пяти месяцев.

Те же деяния, повлекшие по неосторожности тяжкие последствия.

лишение свободы на срок от 3 до 7 лет.

**Статья** 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред

лишение права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет,

либо обязательные работы на срок от 180 до 240 часов,

либо ограничение свободы на срок до 2 лет.

То же деяние, повлекшее по неосторожности тяжкие последствия.

лишение свободы на срок до 4 лет.