
УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР
по ГО и ЧС Вологодской области

Преподаватель БОУДПО Вологодской области

«УМЦ по ГО и ЧС Вологодской области»

Носков Владимир Валентинович

тел : 72-45-32

УГРОЗА КИБЕРТЕРРОРИЗМА. ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ. ОСНОВНЫЕ МЕРЫ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ В ЦЕЛЯХ ПРЕДОТВРАЩЕНИЯ КИБЕРТЕРРОРИЗМА. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ.

Понятия «кибертерроризма» и «кибербезопасности». Возможности сети Интернет для осуществления террористических актов. Примеры хакерских атак как способа реализации экстремистских и террористических действий.

Определить понятие ***«компьютерный терроризм»*** – достаточно трудная задача, поскольку нелегко установить четкую границу для отличия его от информационной войны и информационного криминала. Еще одна трудность состоит в том, что необходимо выделить специфику именно этой формы терроризма. Само понятие ***«кибертерроризм»*** образовано слиянием двух слов: ***«киберпространство»*** (сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности) и ***«терроризм».***

Исходя из основного понятия терроризма (***ст. 3 Федерального Закона № 35-ФЗ «О противодействии терроризму***) и сочетания его с виртуальным пространством, можно вывести следующее определение.

Кибертерроризм – это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанными с устрашением населения и (или) иными формами противоправных насильственных действий, совершаемые в информационном и (или) киберпространстве с использованием компьютерных технологий.

Соответственно, под термином ***«кибертеракт»*** можно понимать ***действия по дезорганизации информационных систем, устрашающие население и создающие опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях.***

Трансграничный характер киберпространства, его зависимость от сложных информационных технологий, активное использование площадок и сервисов киберпространства всеми группами граждан России определяют новые возможности, но при этом и развивают новые угрозы личности, обществу и государству.

Угроза информационной безопасности Российской Федерации - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере. («Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерациот 05.12.2016 г. № 646)

Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

(***Основы государственной политики российской федерации в области международной информационной безопасности на период до 2020 года***)

В официальных российских документах в области информационной безопасности термин «кибербезопасность» не выделяется из объема понятия «информационная безопасность» и не используется отдельно.

Информационная безопасность Российской Федерации *- состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. («Доктрина информационной безопасности Российской Федерации»* утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646)

В одном из неофициальных документов Совета Федерации Федерального Собрания Российской Федерации – ***проекте «Концепции Стратегии кибербезопасности Российской Федерации»*** - ***кибербезопасность*** понимается, как более узкое по смыслу понятие, чем ***информационная безопасность*** и означает ***совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.***

Интернет как технология обязан своим рождением американским военным. В начале 70-х годов прошлого столетия специалисты Пентагона работали над тем, как сделать военные коммуникации неуязвимыми для ядерной атаки (со стороны Советского Союза). Выход был найден в создании децентрализованной сети подключенных друг к другу компьютеров, где вывод из строя достаточно большого количества узлов, составляющих сеть, не влияет на доставку данных. Уже в конце 80-х Интернет был открыт для коммерческого использования.

Сегодня можно говорить о том, что Интернет охватывает все страны мира, так как благодаря применению новых технологий (использование мобильных спутниковых устройств связи) к сети Интернет можно подключиться из любой точки земного шара. Если же говорить о развернутой инфраструктуре, то в таком контексте Интернет охватывает сегодня более 150 стран мира. В России, по разным оценкам, число пользователей Интернета составляет от 3,5 до 8 миллионов человек.

При этом Интернет по-прежнему остается неким виртуальным «свободным пространством», демократией в высшем своем проявлении, где каждый волен свободно излагать свои взгляды. Транснациональные террористические организации, в том числе и «Аль-Каида», по достоинству оценили демократизм практически никем не контролируемой Сети и активно используют ее как для пропаганды своих взглядов, так и для непосредственной подготовки террористических актов.

Возможности Интернета по распространению информации и его информационному воздействию не меньше, чем у традиционных средств массовой информации, таких как газеты, радио и телевидение. Обширные возможности Интернета активно используются различными экстремистскими и террористическими организациями для пропаганды расовой, религиозной и других форм нетерпимости.

Цели использования террористами сети Интернет весьма разнообразны:

- обеспечение доступа к средствам массовой информации и пропаганда террористической деятельности;

- создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация данных о времени и встрече людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., то есть оказание синергетического воздействия на деятельность групп, поддерживающих террористов;

- использование Интернета для обращения к массовой аудитории с целью сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов;

- Всемирная паутина способна инициировать психологический терроризм. С помощью Интернета террористические организации сеют панику, вводят в заблуждение, приводят к разрушению эмоциональных и поведенческих установок индивида.

Сегодня в Интернете функционирует большое количество информационных ресурсов (сайтов), способствующих развитию ксенофобии и экстремизма. Условно такие **сайты можно разделить на четыре основные группы**.

1. Сайты, непосредственно распространяющие идеи экстремизма, сепаратизма и терроризма. В частности, через такие ресурсы международные террористические организации практически беспрепятственно осуществляют пропаганду радикальных течений ислама, проповедующих идеи джихада и борьбы с «неверными».

2. Информационные ресурсы, осуществляющие информационную и финансовую поддержку представителей международных террористических организаций. Эти сайты призывают к совершению террористических актов, пропагандируют сепаратизм, религиозную нетерпимость и межнациональную рознь.

3. Сайты, разжигающие ксенофобию на основе расовой или национальной принадлежности. К ним, в частности, относятся интернет-ресурсы антисемитского характера.

4. Интернет-ресурсы справочного характера, напрямую не призывающие к противоправной деятельности.

Примеры хакерских атак как способа реализации экстремистских и террористических действий.

Вирус Stuxnet 2010 года: блокирована ядерная программа Ирана

Эта вирусная программа, которая весила менее одного мегабайта, была запущена в сеть иранских ядерных заводов. Когда вирус достиг точки назначения, он взял под контроль всю систему. Затем он приказал пяти тысячам урановых центрифуг вращаться без контроля, внезапно останавливаться, а затем снова начинать вращение, параллельно посылая отчеты о том, что все в порядке. Эта хаотичная манипуляция продолжалась в течение 17 месяцев, заставляя заводы жить своей собственной жизнью, а рабочих и ученых сомневаться в собственном рассудке. И на протяжении всего этого времени никто не знал, что происходит. Коварная и скрытная атака принесла больше вреда, чем если бы эти центрифуги были бы просто уничтожены. Вирус вел тысячи специалистов по неправильному пути в течение полутора лет, потратив тысячи часов работы и урановые ресурсы, оцениваемые миллионами долларов. Этот хак запомнился как размахом, так и хитростью: вирус атаковал ядерную программу страны, которая находилась в состоянии конфликта с США и другими мировыми державами, а также он обманывал тысячи научных работников в течение полутора лет, пока он скрытно выполнял свою грязную задачу.

Spamhaus 2013 года: крупнейшая DDOS-атака в истории

DDOS-атака — это, по сути, поток данных. Используя десятки компьютеров, которые повторяют одинаковый сигнал с большой частотой и на высоком уровне шума, хакеры буквально затапливают и перегружают компьютерные системы в интернете. В марте 2013 года эта конкретная DDOS-атака оказалась настолько большой, что она замедлила работу всего интернета во всем мире, а также полностью отключило его в некоторых частях мира на целые часы.

Основные принципы кибербезопасности организации.

Организация безопасного доступа к сети Интернет с рабочих мест в организации.

Контент-фильтрация информации.

Использование современного программного обеспечения для защиты данных организации

Основные требования к безопасности при работе с программным обеспечением, при работе в сети Интернет.

.

В отличие от обычного террориста, который для достижения своих целей использует взрывчатку или стрелковое оружие, кибертеррорист использует современные информационные технологии, компьютерные системы и сети, специальное программное обеспечение, предназначенное для несанкционированного проникновения в компьютерные системы и организации удаленной атаки на информационные ресурсы жертвы. В первую очередь –это ***компьютерные программные закладки и вирусы***, в том числе и сетевые, осуществляющие съём, модификацию или уничтожение информации, так называемые «логические бомбы», «троянские» программы и иные виды информационного оружия.

В киберпространстве могут быть использованы ***различные приемы для совершения террористического акта***:

- нанесение ущерба отдельным элементам киберпространства, разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств;

- хищение или уничтожение информационного, программного и технического ресурсов киберпространства, имеющих стратегическую значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок;

- воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления; раскрытие и угроза опубликования закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодов шифрования, принципах работы систем шифрования;

- захват каналов телекоммуникационного вещания с целью распространения дезинформации, слухов, демонстрации и мощи террористической организации и объявления своих требований;

- уничтожение и активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммуникации, воздействие на операторов, разработчиков информационных и телекоммуникационных систем с целью совершения ими перечисленных выше действий.

Обеспечение информационной безопасности *- осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.*

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.

(«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646)

Система обеспечения информационной безопасности *- 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 законодательством Российской Федерации 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.

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

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

(«Доктрина информационной безопасности Российской Федерации»
утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646)

Организационную основу системы обеспечения информационной безопасности составляют: *Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.*

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

(«Доктрина информационной безопасности Российской Федерации»
утверждена Указом Президента Российской Федерацииот 05.12.2016 г. № 646)

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-разыскного, 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.

(«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерациот 05.12.2016 г. № 646)

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

(«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерациот 05.12.2016 г. № 646)

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

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

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

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

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

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

(«Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента Российской Федерациот 05.12.2016 г. № 646)

Обладателем информации *может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.*

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Федеральный закон от 27.07.2006 № 149-ФЗ « Об информации, информационных технологиях и о защите информации (в ред. от 19.07.2018)

Организация безопасного доступа к сети Интернет с рабочих мест в организации ***включает в себя*** комплекс правовых, организационных и технических мероприятий, 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; 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;

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

Федеральный закон от 27.07.2006 № 149-ФЗ « Об информации, информационных технологиях и о защите информации (в ред. от 19.07.2018)

К правовым мероприятиям относится разработка в организации нормативно-правовых документов, которые определяют:

- порядок подключения автоматизированных рабочих мест сотрудников предприятия к сети Интернет;
- назначение доступа к ресурсам сети Интернет;
- регистрацию пользователя;
- ограничения при работе в сети Интернет;
- обращение в другие организации от имени учреждения;
- контроль использования ресурсов сети Интернет.

Одним из таких документов может быть «Положение о порядке подключения и работы автоматизированных рабочих мест сотрудников предприятия в сети Интернет».

К организационным мероприятиям относится мероприятия которые:

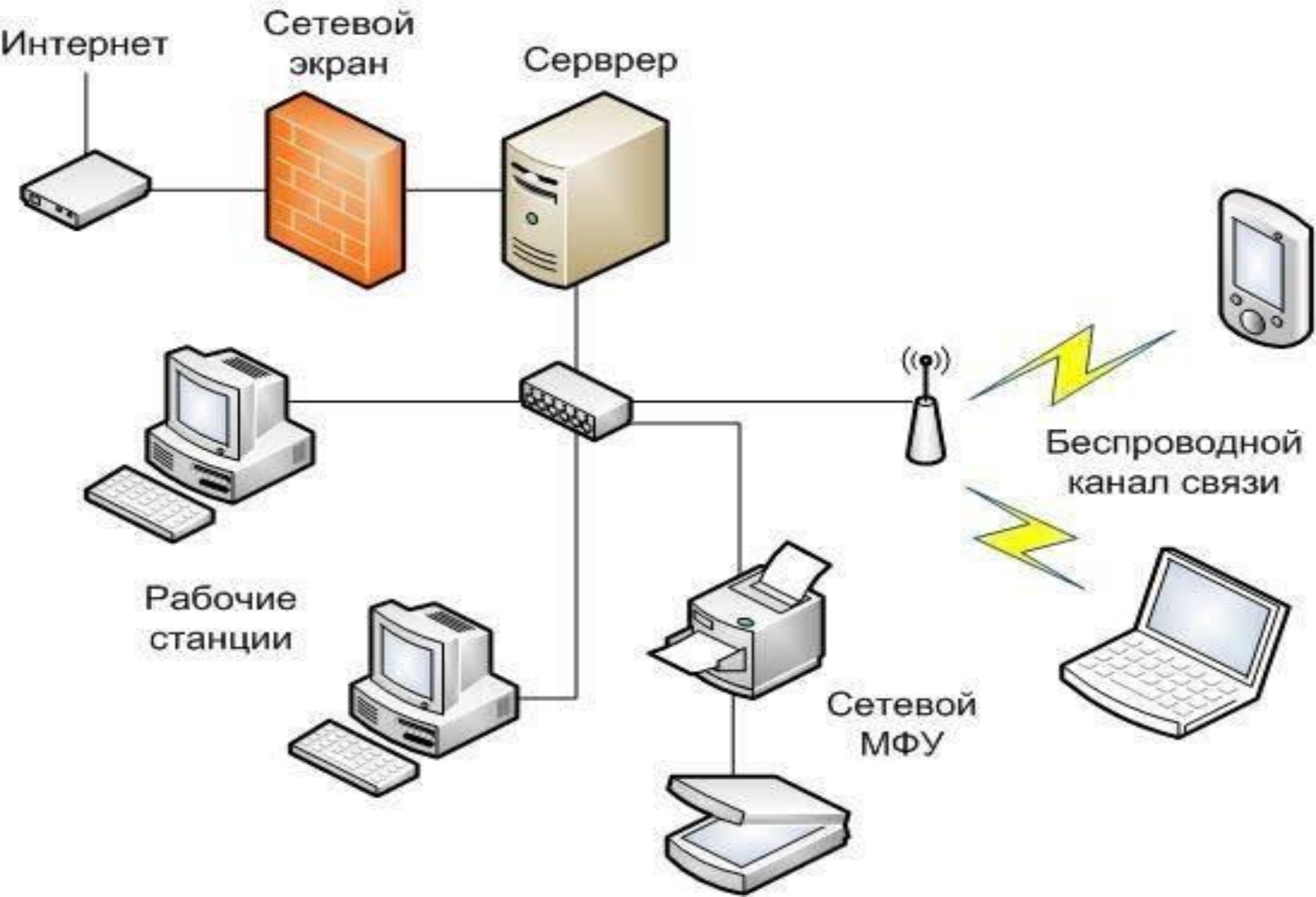
- определяют порядок подключения рабочих мест сотрудников к международной сети Интернет и регламентируют использование сети Интернет в учреждении;
- направлены на повышения эффективности работы сотрудников, использующих электронные информационные ресурсы глобальной сети Интернет, и уровня информационной безопасности локальной информационно-вычислительной сети учреждения;
- устанавливают постоянный контроль и спецификацию видов информации, к которой разрешен доступ тому или иному работнику.

К техническим мероприятиям относится мероприятия по выбору и установке технических устройств и информационных технологий (аппаратно-программных средств) которые позволяют осуществлять:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа (контент-фильтрация информации);
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы;

управление конфигурацией информационной системы.

Пример подключения АРМ учреждения к сети Интернет



В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов сети Интернет особое значение приобретает информационная безопасность организаций, предприятий и учреждений, и в первую очередь образовательных учреждений для детей и молодёжи.

Для этих целей используется программа ограничения веб-контента (англ. Content-control software или web filtering software), которая позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра. Так называемый контент-фильтр.

Контент-фильтр – это устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определённым сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра.

Контент-фильтр работает по статистическому принципу, то есть подсчитывает заранее определённые слова текста и определяет категорию, к которой относится содержимое сайта.

Целью таких устройств или программ является ограничение доступа в Интернет для школ, предприятий, религиозных организаций и т. д. Чаще всего контент-фильтры используются для ограничения доступа для детей и подростков, в учебных заведениях, библиотеках и на рабочих местах в различных учреждениях, а также игровых клубах и интернет-кафе.

Программные средства защиты информации включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.

Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

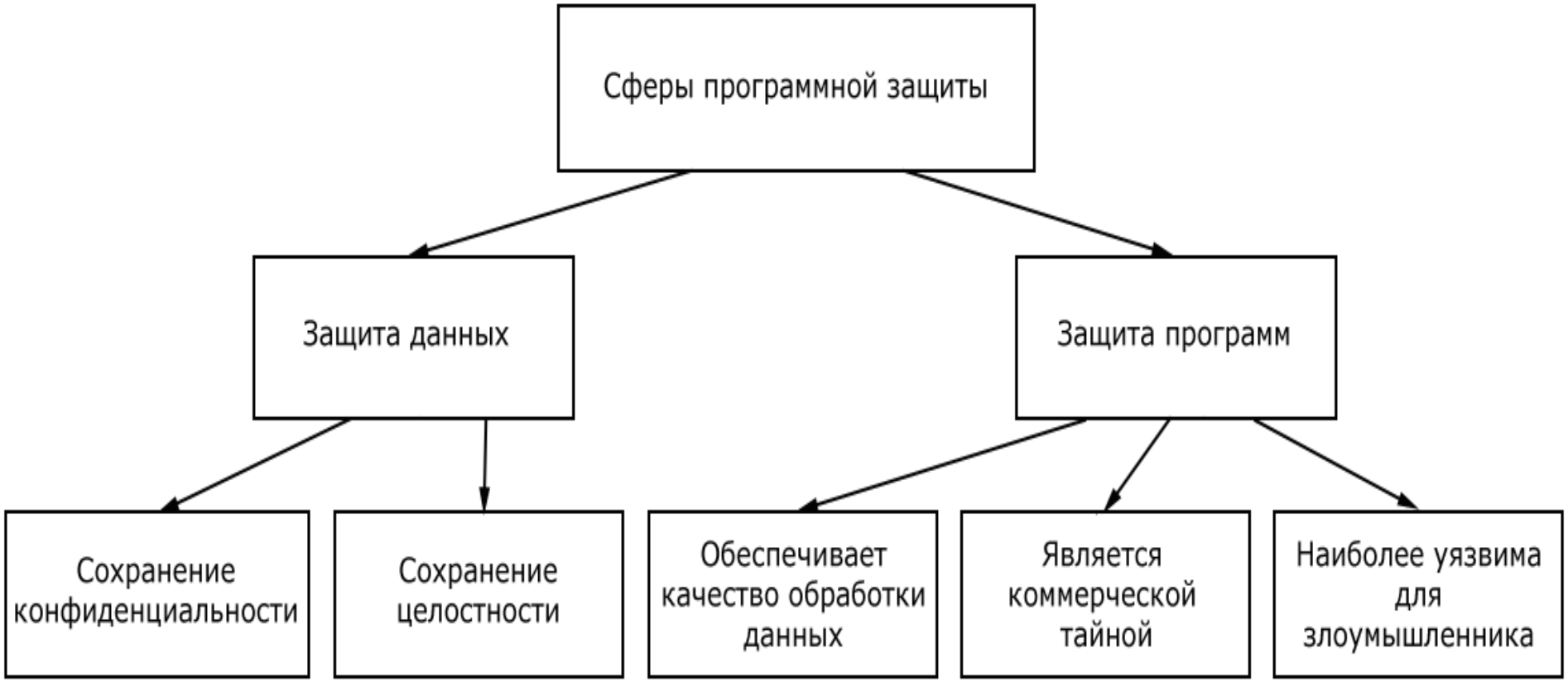
Защита на уровне аппаратуры и программного обеспечения предусматривает управление доступом к вычислительным ресурсам. Защита на уровне данных направлена на защиту информации при обращении к ней в процессе работы и на защиту информации при ее передаче по каналам связи.

Средства регистрации, как и средства контроля доступа, относятся к эффективным методам защиты от НСД. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации – обнаружить уже совершенные действия.

Одна из задач обеспечения безопасности информации для всех случаев пользования ЭВМ является ***защита информации от разрушения***, которое может произойти при подготовке и осуществлении каких-либо восстановительных мероприятий.

Особую опасность представляют ***программы-вирусы***, которые создаются для нарушения работы компьютеров – вплоть до стирания информации.

Для обнаружения и удаления вирусов служат ***антивирусы***. Они подразделяются на специализированные и универсальные. Различие заключается в том, что специализированные антивирусы могут бороться только с уже написанными вирусами, а универсальные – и с еще не написанными. Из универсальных антивирусов большое распространение имеют резидентные антивирусы и программы-ревизоры. Кроме того, для защиты от вирусов используется комплекс различных организационных мероприятий.



Основные направления использования программной защиты информации:

защита информации от НСД,
защита программ от копирования,
защита информации от разрушения,
защита информации от вирусов,
защита программ от вирусов,
программная защита каналов связи.

Программные средства защиты информации делятся на:

- встроенные средства защиты информации;

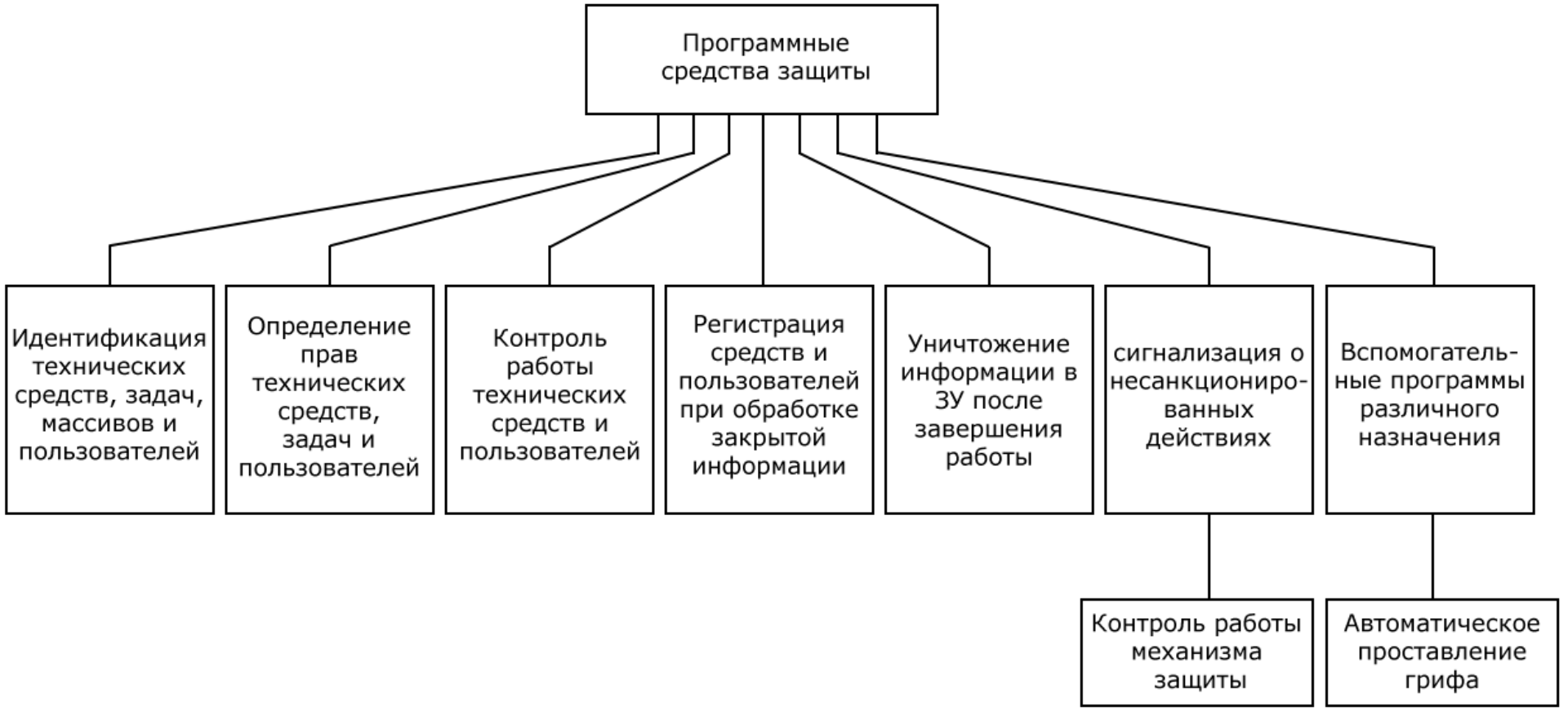
- антивирусные программы (антивирус) - программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики - предотвращения заражения файлов или операционной системы вредоносным кодом;

- специализированные программные средства защиты информации от несанкционированного доступа (обладают в целом лучшими возможностями и характеристиками, чем встроенные средства). Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации.

- межсетевые экраны (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

- proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью - маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях - например, на уровне приложения (вирусы, код Java и JavaScript).

- VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.


Программные средства защиты
Идентификация технических средств, задач, массивов и пользователей
Определение прав технических средств, задач и пользователей
Контроль работы технических средств и пользователей
Регистрация средств и пользователей при обработке закрытой информации
Уничтожение информации в ЗУ после завершения работы
сигнализация о несанкциониро-ванных действиях
Вспомогатель-ные программы различного назначения
Контроль работы механизма защиты
Автоматическое проставление грифа

Защита информации от несанкционированного доступа

Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Особые функции, которые должны осуществляться программными средствами, это:

- идентификация объектов и субъектов,
- разграничение (иногда полная изоляция) доступа к вычислительной технике,
- контроль и регистрация действий с информацией и программами.

В процедурах идентификации используются различные методы:

- простые, сложные и одноразовые пароли,
- обмен вопросами и ответами с администратором,
- средства анализа индивидуальных характеристик,
- ключи, магнитные карты, значки и т.д.,
- специальные идентификаторы или контрольные суммы для аппаратуры.

После идентификации защита осуществляется на 3 уровнях:

- аппаратуры,
- программного обеспечения,
- данных.

Классификация систем защиты от несанкционированного доступа

Системы защиты компьютера от чужого вторжения весьма разнообразны и могут классифицироваться по следующим группам:

- средства собственной защиты, предусмотренные общим программным обеспечением;
- средства защиты в составе вычислительной системы;
- средства защиты с запросом информации;
- средства пассивной защиты и т.д.

Защита информации от копирования

Защита информации от копирования реализуется выполнением ряда функций, являющихся общими для всех систем защиты:

идентификация среды, из которой будет запускаться программа,

аутентификация среды, из которой запущена программа,

реакция на запуск из несанкционированной среды (сводится к выдаче сообщений),

регистрация санкционированного доступа,

противодействие изучению алгоритмов работы системы.

Защита персональных данных работников как один из способов обеспечения кибербезопасности, противодействия совершению возможных террористических актов. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»

Основные нормативно-правовые акты, регламентирующие работу с персональными данными

1. *Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»*
2. *Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»*
3. *Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»*
4. *Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»*
5. *Приказ ФСТЭК РФ от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»*
6. *Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»*
7. *Приказ ФСБ РФ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищённости»*

***Персональные данные** – любая информация, относящаяся прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).*

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Таким образом, делаем вывод, что информация, которая прямо или косвенно не указывает на конкретное физическое лицо персональными данными не является.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

***Хранение персональных данных** должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.*

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Персональные данные, в зависимости от целей их обработки, можно разделить на несколько категорий:

- общедоступные (данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральным законом не распространяются требования соблюдения конфиденциальности);
- специальные (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни);
- биометрические (характеризующие физиологические особенности человека и на основе которых можно установить его личность).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Условия обработки персональных данных

(Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»)

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

3.1) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1.1. Обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом от 27 мая 1996 года N 57-ФЗ "О государственной охране".

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

Постановление Правительства РФ от 5.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Категории информационных систем персональных данных

Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных для 2 - го уровня защищенности персональных данных, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных для 3 -го уровня защищенности персональных данных, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119
«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных для 4 -го уровня защищенности персональных данных, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

СПАСИБО ЗА ВНИМАНИЕ!