ЧУДПО РЦБ

ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«РЕГИОНАЛЬНЫЙ ЦЕНТР БЕЗОПАСНОСТИ»
390010, г. Рязань, ул. Новикова-Прибоя, дом 10, тел. (4912) 38-82-08, 38-76-96 .E-mail: dporzn@yandex.ru

ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАТИЗАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Лекция 2

1. Объекты, подлежащие защите (продолжение).

1. Объекты, подлежащие защите (продолжение).

Объекты информатизации

Автоматизированная система, в том числе АСЗИ, объекты информатизации и их составные части (компоненты) являются объектами информационной инфраструктуры, которые совместно с информационными объектами составляют объекты информационной сферы в соответствии с определением, приведенным в пункте 1 раздела 1 Доктрины информационной безопасности Российской Федерации.

В названной Доктрине информационная сфера определяется **как совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.**

Объекты информатизации

В соответствии с этим определением информационную сферу следует рассматривать как сферу, состоящую из следующих компонентов:

1) объектов;

2) субъектов;

3) системы регулирования отношений, возникающих между субъектами и объектами информационной сферы.

Объекты информатизации

Объектами информационной сферы являются информационные объекты и объекты информационной инфраструктуры, включающие в себя организационно-технические (социо-технические) объекты и технические объекты.

Объекты информатизации

Информационный объект – совокупность информации, определяемой по каким-либо признакам.

Организационно-технический объект – информационная система и (или) информационно-телекоммуникационная система, объект информатизации.

Технические объекты – компоненты организационно-технических объектов, способные функционировать самостоятельно без участия человека или в составе организационно-технических объектов.

1. Объекты, подлежащие защите.

В настоящее время основным видом информационных систем являются автоматизированные системы, т.е. системы, функционирование которых осуществляется при обязательном участии человека.

Процесс функционирования автоматизированных систем происходит в том числе при воздействии вредоносных факторов.

Определение фактора, воздействующего на информацию, приведено в ГОСТ Р 51275 — 99: это **явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.**

Как видно из определения факторы наносят вред защищаемой информации.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

В соответствии с определением, вредоносные факторы способны оказывать вредоносное воздействие на объекты защиты информации. Однако эта способность реализуется не во всех случаях, когда осуществляется воздействие вредоносных факторов на объекты защиты информации. Вредоносный фактор может оказывать вредоносное воздействие лишь при определенных условиях, которые определяются свойствами и состояниями создаваемого, модернизируемого, развиваемого или эксплуатируемого объекта информационной инфраструктуры, субъектов и объектов информационной сферы, а также внешних объектов и субъектов.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Определив условия, в которых будет осуществляться создание, модернизация, развитие или эксплуатация объектов информационной инфраструктуры, можно разделить всё множество вредоносных факторов на два вида:

- вредоносные факторы, которые в определенных условиях не могут оказывать вредоносное воздействие на конкретную совокупность объектов защиты информатизации;

- вредоносные факторы, которые в определенных условиях оказывают вредоносное воздействие на конкретную совокупность объектов зашиты информации.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Факторы второго вида будем для краткости и отличия от факторов первого вида называть вредоносными воздействиями. Выделение среди всего множества факторов, приведенных в ГОСТ Р 51275-2006, вредоносных воздействий, на противодействие которым должна быть направлена защита информации, возможна только при конкретных условиях, в которых осуществляется создание, модернизация, развитие или эксплуатация конкретной совокупности объектов защиты информации.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Определение вредоносных воздействий, на противодействие которым должна быть направлена защита информации в конкретном комплексном объекте защиты информации, в конкретных условиях является важным фактором для обеспечения эффективной защиты обрабатываемой в этом объекте информации. Без определения всей совокупности вредоносных воздействий невозможно определить условия защиты информации и, следовательно, обеспечить эффективную защиту информации на любом объекте информационной инфраструктуры. Для успешного решения задач определения всей совокупности вредоносных воздействий на любой объект информационной инфраструктуры необходимо четко представлять сущность и иметь на основе этой сущности определение понятия вредоносное воздействие на объект информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

На протяжении своего жизненного цикла любой объект информационной инфраструктуры подвергается многократным различным воздействиям, в том числе, вредоносным. В связи с этим важным для правильной организации защиты объекта информационной инфраструктуры от вредоносных воздействий являются сведения, характеризующие эти воздействия как массовые явления, например, как поток заявок в теории массового обслуживания. Всё множество возможных воздействий на объект информационной инфраструктуры, как на стадиях его создания, так и при эксплуатации, можно разделить на два класса в зависимости от их необходимости для реализации объектом информационной инфраструктуры своих функций по обработке информации на штатные воздействия и нештатные воздействия.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Штатными воздействиями будем называть воздействия на объект информационной инфраструктуры, необходимые для выполнения этим объектом своих функций, обеспечивающих его целевое применение в соответствии с проектной документацией на него. Все остальные воздействия на объект информационной инфраструктуры будем называть нештатными воздействиями.

Необходимость воздействия на объект информационной инфраструктуры для выполнения им своих функций является первым классификационным признаком для разделения воздействий на штатные и нештатные.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Объекты информационной инфраструктуры, обрабатываемая в них информация, в соответствии с законодательством Российской Федерации являются объектами отношений физических, юридических лиц, государства и, следовательно, воздействий на них могут причинить и субъектам информационной сферы определенный ущерб. Кроме того, объекты информационной инфраструктуры, в результате оказания на них вредоносных воздействий, могут нанести ущерб окружающей среде. Сумму всех перечисленных ущербов будем называть вредоносной составляющей результата вредоносного воздействия на объект информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Нанесение объекту информационной инфраструктуры определенного ущерба является общим свойством как штатных, так и нештатных воздействий на него. Однако это свойство различно для штатных и нештатных воздействий на объект информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Для вредоносной составляющей результатов любого штатного воздействия на объект информационной инфраструктуры является обязательным:

1) величина ущерба объекта информационной инфраструктуры, как правило, прямо или косвенно определяется в документации на этот объект;

2) величина ущерба не приводит к разрушению как объекта информационной инфраструктуры в целом, так и его компонентов, вызывающему неспособность этого объекта выполнять свои функции (исключением могут являться объекты информационной инфраструктуры, используемые в качестве информационного оружия или его компонентов);

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

3) штатное воздействие на объект информационной инфраструктуры не должно наносить ущерб окружающей среде и (или) субъектам информационной сферы.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Для нештатных воздействий на объект информационной инфраструктуры вредоносная составляющая результата этого воздействия может обладать следующими характерными особенностями:

1) величина ущерба, наносимого объекту информационной инфраструктуры, может иметь любые размеры, в том числе влияющего на возможности полного или частичного, постоянного или временного выполнения этим объектом части или всех своих функций, к разрушению этого объекта в целом или отдельных его компонентов;

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

2) воздействуя на объект информационной инфраструктуры, нештатное воздействие может нанести ущерб субъектам информационной сферы, окружающей среде, причем как при нанесении, так и при не нанесении ущерба самому объекту информационной инфраструктуры.

Таким образом, вредоносная составляющая результата воздействия на объект информационной инфраструктуры является вторым классификационным признаком для разделения воздействий на штатные и нештатные.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Штатные воздействия на объект информационной инфраструктуры кроме нанесения ему некоторого ущерба обеспечивают его функционирование, т.е. результатом штатных воздействий является не только ущерб, но и создание необходимых условий для его целевого применения, что является полезной частью результата воздействия. Поэтому штатные воздействия на объект информационной инфраструктуры не могут рассматриваться в качестве вредоносных воздействий, хотя они и наносят определенный ущерб этому объекту.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Таким образом, в качестве вредоносных воздействий можно рассматривать только нештатные воздействия на объект информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Классификационным признаком для разделения нештатных воздействий на вредоносные и невредоносные должна быть составляющая нештатного воздействия – результат воздействия. Результат некоторых нештатных воздействий на некоторые объекты информационной инфраструктуры, кроме вредоносных составляющей, может содержать некоторые полезные элементы, например, для объекта информационной инфраструктуры. Полученная информация о свойствах вредоносного воздействия при его воздействии на эти объекты при наличии у них адаптивной защиты может быть использована для повышения их защищенности.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Полезную часть результата воздействий на объект информационной инфраструктуры будем называть положительной составляющей результата воздействия. Использование положительной составляющей результата воздействия для классификации нештатных воздействий и определение понятий вредоносное воздействие на объект информационной инфраструктуры является целесообразным, т.к. она не является обязательной для всех нештатных воздействий и ее наличие в результате нештатного воздействия зависит от свойств объекта, на которые воздействия оказываются.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

В качестве классификационного признака для разделения нештатных воздействий на вредоносные и невредоносные необходимо использовать свойство вредоносной составляющей результатов этих воздействий на объект информационной инфраструктуры - величину ущерба, наносимого этому объекту, субъектам информационной сферы окружающей среде.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Будем относить к вредоносным воздействиям нештатные воздействия на объект информационной инфраструктуры, результат которых характеризуется недопустимыми величинами ущерба, наносимого этому объекту информационной инфраструктуры, субъекту информационной сферы, окружающей среде. При этом величины ущерба могут оцениваться как качественными, так и количественными показателями, а также на их основе формироваться единый показатель количественный или качественный величины ущерба. При использовании любых показателей величины ущерба, наносимого нештатным воздействием на объект информационной инфраструктуры, решение вопроса о допустимости или недопустимости значений этих показателей в соответствии с законодательством Российской Федерации относятся к компетенции собственника и (или) оператора объекта информационной инфраструктуры и (или) пользователя, обладателя обрабатываемой в этом объекте информационной инфраструктуры информации.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Ущерб, по своей сути, является результатом взаимодействия двух различных сущностей: с одной стороны, нештатного воздействия, а с другой - объекта информационной инфраструктуры. Следовательно, его величина будет всегда определяться свойствами каждой из двух названных сущностей. Это приводит к неоднозначности решения задачи классификации нештатных воздействий на вредоносные и невредоносные.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Для устранения неоднозначности решения названной задачи следует использовать в качестве классификационного признака нештатных воздействий на объект информационной инфраструктуры величину ущерба, наносимого этому объекту, его собственнику, оператору, пользователю и (или) обладателю обрабатываемой в этом объекте информации, окружающей среде этим нештатным воздействием при условии отсутствия у объекта информационной инфраструктуры встроенных средств защиты информации и защитных функций, а так же отсутствие в системе, в которую входит этот объект, внешних средств защиты и защитных функций. Эту величину ущерба будем называть исходной величиной ущерба. Ущерб, характеризуемый такой исходной величиной будем называть исходным ущербом.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Объекты информационной инфраструктуры могут осуществлять только обработку информации, зафиксированной на каком-либо штатном носителе информации. Объекты информационной инфраструктуры, содержащие в своем составе аппаратные средства обработки информации в процессе своего функционирования могут порождать штатные носители, в которых отображена обрабатываемая информация, а так же переносить на существующие нештатные носители информации.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Получение доступа к нештатному носителю информации не способно нанести ущерб самому объекту информационной инфраструктуры или нарушить его функционирование, но может привести к получению обрабатываемой информации несанкционированным субъектом. Воздействия на нештатный носитель информации с целью получения зафиксированной в нем обрабатываемой информации, всегда является нештатным.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

С учетом всего сказанного сформулируем следующие определения понятия вредоносное воздействие на объект информационной инфраструктуры, выбрав в качестве способа реализации его содержательной части перечисление установленных отличительных особенностей вредоносных воздействий:

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

вредоносное воздействие на объект информационной инфраструктуры – нештатное воздействие на объект информационной инфраструктуры и (или) на нештатный носитель, порождаемый этим объектом в процессе обработки информации и (или) на нештатный носитель (существующий), на который переносится информация, обрабатываемая на объекте информационной инфраструктуры, результатом которого является (может являться) недопустимый исходный ущерб, наносимый самому объекту и (или) его собственнику, оператору, а так же пользователю, обладателю обрабатываемой информации в этом объекте, окружающей среде.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Вредоносные воздействия на объект информационной инфраструктуры необходимо классифицировать на основе свойств, составляющих этих воздействий. Наиболее часто для этого используются свойства следующих составляющих вредоносного воздействия на объект информационной инфраструктуры:

1) участников вредоносного воздействия;
2) цели или целей вредоносного воздействия;
3) объектов вредоносного воздействия;
4) способов и методов реализации вредоносного воздействия;
5) источников вредоносного воздействия;
6) результата вредоносного воздействия.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Участник вредоносного воздействия – субъект (физическое лицо, группа физических лиц), являющихся инициатором и (или) непосредственным участником процесса вредоносного воздействия.

В зависимости от наличия участника вредоносного воздействия на объект информационной инфраструктуры как и факторы, воздействующие на информацию, разделяются на субъективные и объективные.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Субъективное вредоносное воздействие – вредоносное воздействие, инициатором и (или) непосредственным участником которого является субъект (физическое лицо, группа физических лиц).

С точки зрения цели (целей) субъективные вредоносные воздействия подразделяются на преднамеренные и на непреднамеренные.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Преднамеренное субъективное вредоносное воздействие – субъективное вредоносное воздействие, участник (участники) которого при реализации процесса вредоносного воздействия стремится (стремятся) к достижению какой-либо цели (целям).

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Цель (цели) участника вредоносного воздействия могут быть как заранее намеченные и неизменные, так и изменяющиеся в процессе вредоносных воздействий.

Непреднамеренное субъективное вредоносное воздействие - субъективное вредоносное воздействие, участник которого участвует в процессе этого воздействия без какой-либо цели, непреднамеренно (по ошибке, по незнанию и т.п. причинам).

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Объект вредоносного воздействия – совокупность объектов защиты информации, на которую непосредственно или опосредовано оказывается вредоносное воздействие.

Совокупность объектов защиты информации, подвергающихся непосредственному или опосредованному вредоносному воздействию будем называть зоной оказания вредоносного воздействия.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

В зависимости от ее размеров и объектов, входящих в нее, вредоносные воздействия можно разделить на:

1) глобальные вредоносные воздействия, воздействующие на объект информационной инфраструктуры в целом;

2) локальные вредоносные воздействия, воздействующие на отдельные подсистемы объекта информационной инфраструктуры;

3) объектовые вредоносные воздействия, воздействующие на отдельные объекты защиты информации в составе объекта информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

По способам и методам реализации вредоносные воздействия можно разделить на информационные, программно-математические, физические, организационные. Примерами вредоносных воздействий, использующих информационные способы и методы реализации являются:

1) нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

2) осуществление несанкционированного доступа к информационным ресурсам и их противоправное использование;

3) хищение информационных ресурсов из банков и баз данных;

4) нарушение технологии обработки информации и т.п.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Примерами вредоносных воздействий, использующих программно-математические способы и методы реализации, являются:

1) внедрение в аппаратные и программные изделия компонентов, реализующих функции, непредусмотренные или неописанные в документации на эти изделия;

2) разработка и внедрение программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации и т.п.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Примерами вредоносных воздействий, использующих физические способы и методы реализации, являются:

1) уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

2) уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

3) хищение программных или аппаратных ключей и средств криптографической защиты информации;

4) внедрение электронных устройств перехвата информации в средствах связи и телекоммуникационных системам, а также в служебных помещениях и т.п.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Примерами вредоносных воздействий, использующих организационные способы и методы, являются:

1) невыполнение требований нормативных правовых актов в области защиты информации;

2) невыполнение требований, установленных в эксплуатационной документации на объект информационной инфраструктуры и т.п.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

По местонахождению источника вредоносного воздействия эти воздействия следует различать на внутренние вредоносные воздействия и внешние вредоносные воздействия.

Внутреннее вредоносное воздействие – вредоносное воздействие, источником которого являются объекты и (или) субъекты, находящиеся в пределах контролируемой зоны объекта информационной инфраструктуры.

Внешнее вредоносное воздействие – вредоносное воздействие, источником которого являются объекты и (или) субъекты, находящиеся за пределами контролируемой зоны объекта информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

В зависимости от результата вредоносные воздействия разделяются:

- на вредоносные воздействия, результатом которых является утечка защищаемой информации;

- на вредоносные воздействия, результатом которых является непосредственное или опосредованное воздействие на защищаемую информацию.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Кроме разделения вредоносных воздействий, в зависимости от свойств их составляющих, важной является классификация вредоносных воздействий по интервалу времени, в течение которого они могут воздействовать на объект информационной инфраструктуры.

Обычно, в качестве интервалов воздействия выбирают стадии и (или) этапы жизненного цикла объекта информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Понятия вредоносное воздействие на объект информационной инфраструктуры, сущность и определение которого были рассмотрены, а также рассмотренное разделение вредоносных факторов определяют сущность понятия угроза безопасности информации как некоторую опасность объекта информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Эта опасность определяется совокупностями свойств двух сущностей:

1) условий, в которых осуществляется создание, модернизация, развитие или эксплуатация объекта информационной инфраструктуры;

2) вредоносных воздействий на объект информационной инфраструктуры.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Поэтому понятие угроза безопасности информации можно определить следующим образом:

угроза безопасности информации – возможность оказания вредоносного воздействия на объект информационной инфраструктуры, осуществляющий обработку это информации.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Результатом реализации угрозы безопасности информации является оказание вредоносного воздействия на информацию, обрабатываемую в объекте информационной инфраструктуры или на другие его компоненты, приводящего к изменению одной или более характеристик безопасности информации, обрабатываемой в этом объекте.

Вредоносное воздействие на объекты информационной инфраструктуры и угрозы безопасности информации

Поэтому в качестве классификации угроз безопасности информации целесообразно использовать те же признаки классификации, что и для вредоносных воздействий. Единственной дополнительной характеристикой для классификации угроз безопасности информации необходимо выбрать меру осуществимости реализации угрозы. Она может быть как качественной, так и количественной.

В качестве количественной меры осуществимости реализации угроз безопасности информации целесообразно использовать вероятность или частоту ее реализации.