МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

МГУ

Кафедра «Юриспруденция»

**КУРСОВАЯ РАБОТА**

**по курсу «Уголовное право»**

**на тему «Уголовное наказание за диверсию»**

Выполнил студент

2 курса

Перова Екатерина

Санкт Петербург

2007

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ 3

ГЛАВА 1. ПОНЯТИЕ О ДИВЕРСИИ 5

1.1. Характеристика понятия 5

1.2. Предмет диверсии по уголовному кодексу РФ 7

1.3. Классификация диверсий 7

ГЛАВА 2. ДИВЕРСИЯ: ТОЧКИ ЗРЕНИЯ И СУЖДЕНИЯ 13

2.1. Уголовное наказание за диверсию с субъективной и объективной точек зрения 13

2.2. Виды суждений о диверсии 17

ГЛАВА 3. ПРОБЛЕМА ДИВЕРСИИ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ 18

ГЛАВА 4. РЕАЛЬНЫЕ ПРИМЕРЫ ДИВЕРСИЙ 23

ЗАКЛЮЧЕНИЕ 29

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 31

**ВВЕДЕНИЕ**

Прежде слово «диверсия» не имело специфического смысла, появившегося при советской власти («шпион и диверсант»). Диверсией называлась операция, целью которой являлась не прямая победа над неприятелем, а причинение ему такого ущерба, который способствовал бы его поражению в будущих битвах. Периодические бомбардировки Ирака — типичный пример диверсионной войны: избегать генерального сражения, а вместо того устраивать смелые рейды по неприятельским тылам. Более того. Все разговоры последнего десятилетия об абсолютном военном превосходстве передового Запада базировались почти исключительно на опыте диверсий против Саддама Хусейна. Лидер наступившего XXI века Буш счел нужным лишний раз показать, что отныне международное право (в американском толковании, естественно) обрело так недостававшую ему прежде абсолютную санкцию в виде несокрушимой военной мощи, для чего и произвел очередную диверсию.

Само по себе это понятие было введено в состав уголовного законодательства нашей страны еще в 1927 году Положением «О преступлениях государственных», в 9 статье которого это преступление определялось как «разрушение или повреждение с контрреволюционной целью, взрывом, поджогом или иными действиями, железнодорожных или иных путей и средств сообщения, средств народной связи, водопровода , общественных складов и других сооружений или государственного или общественного имущества». В целом подобное определение легко объясняется временем его существования – временем всеобщей борьбы с контрреволюционерами. В 1958 году принимается новый Закон СССР «Об уголовной ответственности за государственные преступления» и трактовка термина «диверсия» изменяется: более подробно перечислены действия, составляющие объективную сторону этого преступления (в том числе включены массовые отравления, распространение эпидемий и эпизоотий), уточнено содержание цели – она отныне определена не как контрреволюционная, а как цель ослабления Советского государства. На данный момент официальное определение понятия «диверсия» заложено в части 1 статьи 281 Уголовного кодекса РФ. Согласно которой диверсия: «Совершение взрыва, поджога или иных действий, направленных на разрушение или повреждение предприятий, сооружений, путей и средств сообщения, средств связи, объектов жизнеобеспечения населения в целях подрыва экономической безопасности и обороноспособности Российской Федерации…». В нынешнее время, активизации различных сепаратистских и террористических организаций рассмотрение термина «диверсия» носит особую ценность.

**ГЛАВА 1. ПОНЯТИЕ О ДИВЕРСИИ**

**1.1. Характеристика понятия**

По своему объему диверсия – понятие общее, т.к. в объеме можно представить множество предметов (множество преступлений-диверсий). Понятие положительно, т.к. оно отражает признаки, которые имеет данное явление. По содержанию понятие конкретно, т.к. мы подразумеваем конкретное явление. Относительно, т.к. в этом понятии один предмет мысли (диверсия) подразумевает существование другого (диверсант), и без него не имеет смысла. Понятие несобирательное, т.к. под ним мы понимаем одно явление (конкретное преступление).

**1.2. Предмет диверсии по уголовному кодексу РФ**

Диверсия направлена на экономическое и оборонное ослабление РФ. Предметом диверсии являются перечисленные в ст. 281 УК материальные объекты, относящиеся к любой форме собственности.

Прежде всего, ими становятся объекты энергетики, оборонной промышленности, транспорта (железнодорожного, воздушного, морского и магистрального трубопроводного), военные объекты и др. В частности, это могут быть: атомные и другие электростанции; линии электропередач и связи; нефте- и газопроводы; шахты; туннели; мосты; плотины; системы тепло- и водоснабжения; склады вооружения, горючего и продовольствия; информационно-вычислительные и телевизионные центры и т.д.

**1.3. Классификация диверсий**

Фактором, затрудняющим разработку понятия и подходов к классификации диверсии, является проблема отождествления диверсии с террором и терроризмом. В словаре иностранных слов «террор»[[1]](#footnote-1) определяется как политика устрашения, подавления политических противников насильственными мерами[[2]](#footnote-2). Статья 205 Уголовного кодекса России предусматривает ответственность за терроризм, - то есть совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного ущерба либо наступление опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза свершения указанных действий в тех же целях. Свою формулировку дает Федеральный закон Российской Федерации «О борьбе с терроризмом» № 130-ФЗ, но она не отличается лаконичностью.

Среди ученых нет единого мнения по вопросу уголовно-правового определения понятия терроризма. Несмотря на определенную общность целей диверсии и терроризма, можно обозначить некоторые принципиальные различия между рассматриваемыми явлениями.

Так, если в статье 281 УК РФ, говорящей о диверсии, дан исчерпывающий перечень преступных действий, то к терроризму, кроме названных непосредственно в статье 205 УК РФ, относятся самые разнообразные иные действия. При диверсии действия преступников направлены на причинение вреда, то при терроризме - на запугивание населения, дестабилизацию обстановки. Цель диверсии состоит главным образом в ослаблении государства, а терроризма - в принуждении к принятию решения или удержанию от его принятия. Диверсант обычно действует тайно, а террорист - демонстративно, привлекает к себе внимание средств массовой информации и населения. Существенным разграничивающим признаком является также ультимативность действий при терроризме.

Под сущностью диверсии следует понимать совокупность признаков, характерных черт и отличительных особенностей, присущих диверсии как военно-политической и правовой категории, и составляющих ее внутреннее содержание. Выделим отличительные признаки диверсионной деятельности как преступного деяния.

Во-первых, отличительной чертой диверсионной деятельности является то, что она направлена на подрыв основ конституционного строя и государственной безопасности. При этом умыслом диверсанта охватывается причинение вреда экономическим интересам и обороноспособности государства.

Во-вторых, диверсионную деятельность отличает скрытый, неочевидный характер исполнения.

В-третьих, отличительной особенностью диверсионной деятельности является необходимость развития агентурной сети, вовлечение в преступную деятельность как можно большего числа лиц.

Очертим круг задач для научного поиска, прежде всего задачу разработки классификаций форм, видов диверсии, средств и способов диверсионной деятельности. Мы предлагаем классифицировать диверсию на:

- экономическую;

- политическую;

- информационную (или идеологическую);

- психологическую (слухи);

- кибердиверсию (электронную диверсию, например, хакерские атаки на сайты органов государственной власти).

Если коротко охарактеризовать экономическую диверсию, то с нашей точки зрения она определяется следующими особенностями. Цель - получение выгоды в результате присвоения экономических ресурсов с нарушением принципа эквивалентности, при этом не исключен полный контроль над экономическими ресурсами региона или государства. Скрытый для общества характер преступлений. Объектом посягательства является экономика государства в целом, отдельные сектора, группы граждан и организаций. Существенный ущерб, причиняемый экономическим интересам государства и общества. Такой диверсии присущ неочевидный, множественный, систематический и длящийся характер, где сложно установить организаторов, исполнителей и пособников преступления и меру их персональной ответственности. Важно учитывать, что диверсионные операции, как правило, тщательно спланированы и участие пособников может быть как прямым, так и косвенным.

В свою очередь частным примером идеологической диверсии является сайт агентства «Кавказ-центр» в сети Интернет. Приведем текст сообщения в разделе «Сотрудничество»: «Независимое международное исламское агентство «Кавказ-центр» приглашает к сотрудничеству журналистов и политических обозревателей. Для того, что бы стать постоянным автором публикаций на сайте KavkazCenter.com необходимо прислать в нашу редакцию авторский материал по любой из следующих тем - «Война на Кавказе», Ичкерия», «Перспективы развития ситуации на Кавказе», «Дагестан», «Ситуация в Закавказских странах», «Российская тематика - Кремль, Путин, олигархи, свобода слова, борьба за власть, перспективы Путина, российская армия, спецслужбы и др.», «Ближний Восток», «Исламский мир», «Афганистан», «Политика США», «Ситуация и перспективы в Центральной Азии», или на любую свободную политическую тему, затрагивающую важные аспекты жизни современного мира.»[[3]](#footnote-3)

Факт идеологической диверсии не вызывает сомнений. Некое международное исламское агентство проводит целенаправленную акцию, порочащую российское государство, и осуществляет открытый наем журналистов и политических обозревателей для совершения преступных действий информационного характера против России.

Особым, недавно появившимся видом диверсий являются диверсии в отношении компьютеров и компьютерных сетей. Распространение Интернета открыло массу возможностей, как в сфере пропаганды, так и непосредственно в сфере вооруженной борьбы. Способы совершения компьютерных преступлений целесообразно подразделять на три группы: способы непосредственного доступа к компьютерной информации; способы удаленного доступа к компьютерной информации; способы распространения технических носителей информации, содержащих вредоносные программы для ЭВМ.

Деление диверсии на формы, (как и любая другая классификация) носит в известной степени условный характер, но выделение конкретных признаков тех или иных форм диверсии необходимо для придания большей целенаправленности и систематизации правотворческой и правоприменительной деятельности в этой области. Наибольшую опасность с нашей точки зрения представляют собой следующие формы диверсии:

Использование в диверсионных целях взрывных устройств; оружия, в том числе биологического, химического, радиационного.

Использование служебного, общественного положения или должностных полномочий.

Использование информации, представляющей государственную тайну.

Хищение секретной информации.

Использование средств массовой информации, в том числе Интернет, специальной литературы.

Использование коммерческих, общественных и религиозных организаций.

Провокация военных, религиозных, межэтнических конфликтов.

Финансирование диверсионной деятельности.

Вовлечение в диверсионную деятельность граждан и организаций (вербовка агентов, создание агентурных сетей).

Диверсионная война.

Список не является исчерпывающим.

Следует отметить, что главной целью акта диверсии по действующему законодательству является умышленное поражение того или иного элемента экономической безопасности или обороноспособности государства. Однако, мы полагаем, что цели диверсий не ограничиваются указанными в законе объектами. Многие диверсии направлены не только на подрыв экономики и обороноспособности страны, но и на разжигание национальной и религиозной вражды и другие опасные цели. Диверсионная деятельность может быть направлены на нарушение территориальной целостности государства и дестабилизацию политической обстановки. Многочисленные признаки этого явления наблюдаются в настоящее время на территории Чеченской Республики.

Таким образом, диверсия может иметь длящиеся во времени цели и включать в себя не только единичные, но и массовые, неоднократные, систематические акции. В связи с вышеизложенным мы полагаем, что статья 281 УК РФ нуждается в существенной корректировке и дополнениях. В частности в законе следует уточнить виды и формы диверсии, разграничить диверсии по масштабам и последствиям, определить границы материального ущерба, причиненного диверсионной деятельностью, как отдельных лиц, так и организаций, меры ответственности за ущерб от диверсий в любой форме; включить в закон и раскрыть такие понятия, касающиеся объективной и субъективной стороны данного преступления, как «диверсионная операция», «диверсионная деятельность», «диверсионная война», «агент влияния», «агентурная сеть», «диверсионная группа», «финансирование диверсионной деятельности». Следует ввести в закон специальные нормы, предусматривающие повышенную ответственность государственных служащих-организаторов, пособников, подстрекателей и исполнителей диверсионных операций. Кроме того, необходима ясность в классификации разнообразных средств, используемых диверсантами: взрывные устройства, оружие, информация, компьютерные вирусы, поджоги и другие, а также способов диверсионной деятельности.

**ГЛАВА 2. ДИВЕРСИЯ: ПРЕДМЕТ И СУЖДЕНИЯ**

**2.1. Уголовное наказание за диверсию с субъективной и объективной точек зрения**

Объективная сторона диверсии довольно подробно описана законодателем. Диверсия осуществляется путем взрыва, поджога или иных действий, направленных на разрушение или повреждение предприятий (например, фабрики, заводы), сооружений (например, электростанция, трубопровод), путей и средств сообщения (например, железнодорожный путь), средств связи (например, линии электропередачи), объектов жизнеобеспечения населения (например, систем водоснабжения) с определенной целью.

Таким образом, объективная сторона диверсии заключается в действиях, направленных на разрушение и повреждение указанных в статье объектов.

Разрушение - полное выведение объекта из строя, когда его восстановление невозможно или нецелесообразно.

Повреждение предполагает частичное выведение объекта из строя при наличии возможности его ремонта и восстановления.
В ст. 281 УК указаны конкретные способы, которыми осуществляются разрушения или повреждения. Это - взрыв, поджог, иные действия. Законодатель не дает исчерпывающего перечня способов совершения диверсии. Но, как правило, они общеопасны, приводят к быстрому результату, серьезному, а иногда непоправимому ущербу экономике и обороноспособности страны.

Законодатель сформулировал состав диверсии по типу формальных составов. Это преступление признается оконченным с момента совершения действий, направленных на разрушение и повреждение определенных объектов. Характер же действий (способ) определен законодателем: взрыв, поджог, иные действия, т.е. затопление, отравление питьевых водохранилищ, устройство обвалов, аварий и пр. С момента осуществления таких действий преступление признается оконченным независимо от того, были разрушены или повреждены или нет указанные в статье объекты.
Квалифицированным видом диверсии является совершение ее организованной группой (ч. 2 ст. 281 УК). Организованная группа - это устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений (ч. 3 ст. 35 УК).

С субъективной стороны преступление совершается только с прямым умыслом и специальной целью. Умыслом виновного охватываются осознание характера и опасности своих действий и желание разрушить или повредить определенные объекты, используя при этом общеопасный способ. Субъект действует со специальной целью - подрыв экономической безопасности и обороноспособности России. Для установления цели диверсии следует учитывать важность выводимого из строя объекта, возможные последствия этого, реальный ущерб экономике и обороноспособности страны, причиненный действиями диверсанта, и т.д.

Мотивы диверсии различны (политические, националистические, корыстные и др.) и на квалификацию содеянного не влияют, но должны учитываться при индивидуализации наказания. Субъектом диверсии могут быть гражданин России, иностранный гражданин, лицо без гражданства. Если действия, подпадающие по своим объективным признакам под понятие диверсии, совершают лица в возрасте от 14 до 16 лет, они должны нести ответственность за фактически совершенные деяния (ст. 20 УК), например, умышленное уничтожение имущества (ст. 167 УК), приведение в негодность транспортных средств и путей сообщения (ст. 267 УК) и пр.

При совершении диверсии по заданию иностранного государства, иностранной организации или их представителей содеянное квалифицируется по совокупности ст. 275 (государственная измена) и ст. 281 УК.

Определенное сходство имеет диверсия с таким преступлением против общественной безопасности, как терроризм (ст. 205 УК), который также осуществляется путем взрыва, поджога или иных действий, создающих угрозу гибели людей, причинение значительного материального ущерба и пр. Разграничение диверсии и терроризма должно проводиться по субъективной стороне - по цели совершения этих преступлений. При диверсии цель - подрыв экономической безопасности и обороноспособности страны путем выведения из строя ключевых хозяйственных и оборонных объектов. Цель терроризма - нарушение общественной безопасности, устрашение населения, воздействие на принятие нужного террористам решения органами власти. Как правило, терроризм направлен против жизни и здоровья людей, а диверсия - на выведение из строя ключевых объектов экономики и обороноспособности. Гибель людей обычно является побочным результатом диверсионного акта. Поэтому в случаях, когда гибель людей при диверсии охватывалась умыслом виновного, его ответственность наступает по совокупности ст. 105 и ст. 281 УК.

В некоторых случаях может возникнуть вопрос о критериях разграничения диверсий и таких преступлений, как умышленное повреждение или уничтожение имущества (ст. 167 УК), уничтожение или повреждение лесов (ст. 261 УК), приведение в негодность транспортных средств или путей сообщения (ст. 267 УК). Критерием разграничения в таких случаях являются направленность действий (различие в родовых, видовых и непосредственных объектах посягательства), а также субъективная сторона, а именно цель совершения указанных действий, которая неразрывно связана и определяет направленность (объект) деяния. Только при диверсии имеется цель подрыва экономической безопасности и обороноспособности.

Таким образом, акции, проведенные 11 сентября в США, по объективной стороне можно отнести к диверсионным акциям.

В октябре 2001 года бывший сотрудник службы внешней разведки КГБ СССР, специалист по антитеррору, председатель исполкома движения «Евразия» Петр Суслов заявил по поводу событий 11 сентября следующее:

«…При проведении теракта его организатор, как правило, берет на себя ответственность и, угрожая повторением акции, выдвигает свои требования. В случае с уничтожением Всемирного торгового центра (ВТЦ) в Нью-Йорке и атаки на Пентагон такую ответственность никто на себя не брал. Только через два с половиной месяца в этом «сознался» руководитель экстремистской исламской организации «Аль-Каида» Усама бен Ладен. Учитывая причастность мусульманских экстремистов к взрывам американского посольства в Бейруте (48 человек убиты, 120 ранены), к атаке камикадзе-одиночки на казармы американских и французских солдат в том же Бейруте (убиты 241 американец и 56 французов) и взрыву американского эсминца «Коэл» в аденском порту (погибли 17 моряков, кораблю нанесены серьезные повреждения), вполне логично объявить его виновным и в сентябрьской трагедии. …Для подготовки акции такого масштаба необходимо большое количество людей и по времени – не менее года. При таких сроках и количестве действующих лиц избежать утечки информации о подготовке теракта практически невозможно. Можно с полной уверенностью утверждать, что ни одна из существующих в мире известных террористических организаций на это не способна. Такое под силу лишь спецслужбе большого государства. Странам со слабой экономикой такое не по плечу. …Наконец, последнее. Диверсии проводятся силами особого назначения одного государства против другого только во время войны или в период подготовки к ней. Сразу после теракта Америка в лице президента Буша, бросив лозунг «Кто не с нами, тот против нас!», начала подготовку к войне, заявив, что «США сами определят государства – пособников террористов, с которыми нужно рассчитаться.»[[4]](#footnote-4)

**2.2. Виды суждений о диверсии**

Существует несколько видов суждений о диверсии.

Суждение свойства (атрибутивное) – суждение о признаке предмета.

Пример: диверсия – совершение взрыва, поджога или иных действий, направленных на разрушение или повреждение предприятий, сооружений, путей и средств сообщения, средств связи, объектов жизнеобеспечения населения в целях подрыва экономической безопасности и обороноспособности Российской Федерации.

Суждение с отношениями (реляционное) – суждение, отражающее отношение между предметами.

Пример: диверсия по степени своей общественной опасности стоит выше, чем кража.

Суждение существования (экзистенциональные) – суждение в котором выражается сам факт существования или не существования предмета суждения.

Пример: описание субъективной стороны диверсии существует в Уголовном кодексе РФ.

**ГЛАВА 3. ПРОБЛЕМА ДИВЕРСИИ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Изучение проблем расследования преступлений в сфере государственной безопасности выступает одной из острейших задач современной уголовно-правовой и криминологической науки. Последние трагически события, связанные со взрывами самолетов, у метро «Рижская» в Москве и захватом заложников в г. Беслане свидетельствуют о целенаправленной диверсионно-террористической войне, развернутой на территории Российской Федерации.

При множестве исследований по проблемам государственной, в том числе экономической безопасности категория «диверсия»[[5]](#footnote-5) в правовой науке практически не изучена. До настоящего времени не найдены ответы на вопросы: каковы формы и виды диверсии; каким образом следует определять масштаб диверсионной деятельности; какими способами с ней можно бороться и другие. Не определена сущность таких важных для квалификации диверсии понятий как «диверсионная операция», «диверсионная деятельность», «диверсионная война», «агент влияния» и т.п. Не разработана методология изучения этого явления.

Проблема диверсии не является новой для отечественной уголовно-правовой науки. Классическое определение диверсии в военной науке – это способ нанесения поражения противнику без вступления с ним в непосредственный огневой контакт. Методы и приемы диверсионной войны широко использовались во время Великой Отечественной войны 1941-1945 гг. партизанскими отрядами на оккупированных территориях.

В Уголовном кодексе 1960 года[[6]](#footnote-6) диверсия была включена в состав государственных преступлений, объединивших тридцать шесть составов. Статья 68 УК РСФСР 1960 года понимала под диверсией совершение с целью ослабления Советского государства взрывов, поджогов или иных действий, направленных на массовое уничтожение людей, причинение телесных повреждений либо другого вреда их здоровью, на разрушение или повреждение предприятий, путей и средств сообщения, средств связи либо другого государственного или общественного имущества, а равно совершение в тех же целях массовых отравлений или распространение эпидемий и эпизоотий. Наказание за эти действия предусматривалось суровое, вплоть до смертной казни[[7]](#footnote-7).

К примеру, в советской литературе широко применялся термин диверсия идеологическая, который подразумевал провокационную пропаганду по радио, телевидению, в печати империалистических государств, направленную против социалистических стран. Особая роль в организации идеологических диверсий против СССР отводилась Центральному разведывательному управлению США, а также антисоветским националистским эмигрантским организациям. Среди таких организаций называли: «Национально-трудовой союз», «Закордонное представительство Украинского главного освободительного совета», «Даугавас Ванаги», «Представительство эстонцев в Швеции», «Совет литовцев Америки», «Дашнакцутюн» и другие.

Состав диверсии существовал в Уголовном кодексе РСФСР до 1994 года и был исключен Федеральным законом от 1 июля 1994 г. Предполагалось, что введение в УК Российской Федерации нормы о терроризме поглощает состав диверсии, поскольку их объективные признаки (взрыв, поджог и иные общеопасные действия) совпадают. Но как показала практика, это исключение было необоснованно ни теоретически, ни практически. Законодатель не учел, что норма о терроризме не нацелена на защиту экономических интересов России, которая с начала 90-х годов ХХ века активно включилась в глобальные мировые процессы. Возникновение новых форм собственности в российской экономике, рост числа новых субъектов хозяйственной деятельности, стремительное развитие предпринимательства повлекли за собой изменение системы субъектов обеспечения безопасности, при котором утратили значение прежние подходы к определению государственных преступлений в сфере экономической деятельности. В УК Российской Федерации 1996 г. состав диверсии был восстановлен, но несколько в иной редакции.

В Уголовном кодексе 1996 года было введено новое понятие «Преступления против основ конституционного строя и безопасности государства» и количество составов было сокращено более чем в три раза, сохранилось всего десять составов. Действующий Уголовный кодекс Российской Федерации (статья 281), включил в состав диверсии следующие действия: совершение взрыва, поджога или иных действий, направленных на разрушение или повреждение предприятий, сооружений, путей и средств сообщения, средств связи, объектов жизнеобеспечения населения в целях подрыва экономической безопасности и обороноспособности Российской Федерации. При этом из числа признаков диверсии исключены такие действия, как массовое уничтожение людей, распространение эпидемий и эпизоотии, совершение массовых отравлений. Подчеркнута направленность диверсии на разрушение или повреждение важных народнохозяйственных и оборонных объектов, а также объектов жизнеобеспечения населения. Круг предметов диверсии сужен. Изменена формулировка цели преступления. Если раньше она формулировалась как цель ослабления Советского государства, то теперь речь идет о цели подрыва экономической безопасности и обороноспособности Российской Федерации.

Безопасность определена в статье 1 Закона РФ «О безопасности» как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Экономическую безопасность следует понимать как состояние защищенности важнейших экономических интересов Российской Федерации.

Обороноспособность Российской Федерации означает состояние ее защищенности от возможного нападения внешнего агрессора и включает такие элементы, как экономический и военный потенциал России, боевая подготовка и профессионализм личного состава Вооруженных Сил РФ, мобилизационная готовность гражданского населения и т.п.

Предметом преступления выступают предприятия (заводы, фабрики), сооружения (мосты, плотины, тоннели, электростанции), пути и средства сообщения и другие объекты.

Объективные признаки диверсии выражаются в совершении взрывов, поджогов и иных действий, направленных на разрушение или повреждение предприятий, сооружений, путей и средств сообщения, средств связи, объектов жизнеобеспечения населения.

Взрыв - это сопровождающееся сильным звуком воспламенение чего-нибудь вследствие мгновенного химического разложения вещества и образования сильно нагретых газов. Поджог - намеренное с преступным умыслом вызывание пожара где-нибудь[[8]](#footnote-8).

Под разрушением следует понимать приведение сооружения в полную негодность.

Под повреждением понимается приведение сооружения в частичную негодность и возможность восстановления и ремонта.

Преступление окончено с момента совершения взрывов, поджогов и иных действий, направленных на разрушение или повреждение объектов диверсии. Фактическое разрушение или повреждение объекта не меняет квалификации преступления.

Диверсия совершается только с прямым умыслом и с целью подрыва экономической безопасности и обороноспособности Российской Федерации.

Ответственность за диверсию несет любое лицо, т.е. гражданин Российской Федерации, иностранный гражданин или лицо без гражданства, достигшее шестнадцатилетнего возраста.

Отягчающим обстоятельством при диверсии (ч.2 статья 281 УК РФ) выступает ее совершение организованной группой, т.е. устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Об устойчивости говорит относительно стабильный численный состав преступной группы. Устойчивость может проявляться и в неоднократности однородных преступных действий.

Если диверсию совершает гражданин Российской Федерации по заданию представителей иностранного государства или иностранной организации, его действия следует квалифицировать по совокупности с государственной изменой в форме оказания помощи в проведении враждебной деятельности против России[[9]](#footnote-9).

Важно отметить и тот факт, что субъект преступления может быть специальный – лицо, использующее свое служебное положение для совершения преступления.

**ГЛАВА 4. РЕАЛЬНЫЕ ПРИМЕРЫ ДИВЕРСИЙ**

Приведем элементарный пример простейшей локальной промышленной диверсии, проведенной по отношению к конкретной фирме, которую террористы вполне могут осуществить в качестве демонстрации или акции устрашения. Некая компания наняла «специалиста», который выяснил номера десяти телефонных линий конкурента, купил десять сотовых телефонов и поставил их в режим автодозвона, забив на несколько дней весь входящий трафик компании. Итог для конкурента - потерянные клиенты и значительные убытки. А исполнителям весь «диверсионный акт» обошелся в сумму порядка тысячи долларов.

Решающий шаг в переходе к качественно новому типу диверсионных актов на основе информационных технологий и против информационных сетей и средств хранения и обработки информации произойдет при использовании хорошо известного военным и сотрудникам спецслужб принципа радиоэлектронного подавления (РЭП).

Этот принцип и соответствующая аппаратура с успехом использовались, например, спецподразделениями Израиля при проведении антидиверсионных операций. Так, во время успешной атаки на виллу одного из лидеров палестинского сопротивления Абу-Нидаля в начале 90-х годов прошлого века средства связи и охранные системы были полностью выведены из строя дистанционным воздействием с пролетавшего в отдалении самолета.

В сфере бизнеса одним из первых примеров диверсии нового поколения является взрыв кустарного электронного фугаса в подземном гараже международного бизнес-центра в Нью-Йорке, осуществленный в середине 90-х годов. Он примечателен тем, что основной ущерб был причинен не конкретными разрушениями и человеческими жертвами, а несколькими днями простоя всех офисов небоскреба.

Прямые убытки частных компаний и правительства США оценивались в сотни миллионов долларов, а непрямые, то есть связанные с нарушением ритма работы бизнес-центра и выходящих на него субъектов деловой жизни планеты, не поддаются исчислению. При этом совершенно не пострадали люди и технические средства офисов (компьютеры, факсы, модемы, ксероксы и т.п., стоимость которых составляет менее 10% стоимости всей специфической системы обработки информации), а основной ущерб определялся потерей содержания баз данных - программного обеспечения (часто уникального) и собственно хранимой информации (остальные 90% потерь).

Источниками технических средств для создания аппаратуры РЭП являются промышленные и исследовательские сверхвысокочастотные установки (СВЧ-установки) и приборы, а также военная техника.

Промышленность развитых стран, в том числе и России, выпускает ряд мощных источников СВЧ-излучения, подходящих для самодельной аппаратуры РЭП. Такие источники используются, к примеру, в радиолокации или сушильных агрегатах. Мощность их излучения находится в пределах десятки кВт - единицы МВт, длина волны обычно 10»12 см (это так называемые промышленные частоты).

Проблема создания импульсного источника питания, применение которого может повысить мощность СВЧ-источника на порядок в сравнении с непрерывным режимом работы, и антенного устройства, формирующего поток излучения, может быть решена средним радиоинженером с использованием доступных деталей и узлов. Установка с источником питания в виде дизель-генератора, импульсными конденсаторными батареями и системой охлаждения источника СВЧ-излучения может быть размещена в кузове легкого грузовика типа ГАЗ-66 или «Газель». За ночь, проехав по крупному городу, такой автомобиль может вывести из строя все банки, биржи, узлы связи, базы данных крупных экономических структур, а также телестудии или издательские комплексы.

Объекты, на которые может быть направлен диверсионный удар средствами РЭП, подразделяют на несколько групп. Это спутники телерадиовещания, связные и разведывательные спутники, электронные СМИ (телерадиоцентры и издательские комплексы), а также различные бизнес-центры (банки, биржи и т.д.).

Спутниковые комплексы являются привлекательной мишенью для диверсий из-за их колоссальной значимости в организации сетей глобальной связи и управления. Современный бизнес немыслим без перекачки коммерческой информации международными связными системами типа «Интелсат» или сотовой телефонной связи на основе спутников «Иридий» фирмы «Моторола». При этом следует иметь в виду, что космическая техника очень уязвима к воздействию средств РЭП, практически не ремонтопригодна, не может быть оперативно заменена на орбите.

Перейти к диверсии нового поколения в принципе способна любая из существующих ныне этническо-религиозных или социально-политических группировок, действующих пока «традиционными» способами. Применяться РЭП-аппаратура может как при решении внутригосударственных задач, сепаратистскими движениями (ирландская ИРА, баскская ЭТА и др.), религиозными движениями (алжирские или египетские фундаменталисты), противниками в этническо-религиозных конфликтах (типа боснийского), так и в рамках уже упоминавшегося «международной диверсии».

Обнаружить диверсионную аппаратуру РЭП еще сложнее, чем взрывное устройство, так как особенности ее боевого применения делает невозможным организацию оперативного преследования и анализа на месте теракта, ведь все средства связи, охраны и видеоконтроля выходят из строя вместе с основной мишенью - компьютерами и базами данных.

Исключительные возможности для развития информационных диверсий появились в связи с взрывным развитием сети Интернет, массовым и быстрым переходом банков, финансовых и торговых компаний на компьютерные операции с использованием разветвленных по всему миру электронных сетей.

Главным действующим лицом в этой ситуации становится не вооруженный боевик или фанатик-самоубийца, а компьютерные взломщики - хакеры, о характере и методах, деятельности которых наслышан любой мало-мальски образованный человек.

Хакеры способны узнать секретную информацию, изменить или стереть ее. Появившись одновременно с интернетом, поначалу они интересовались лишь слабыми местами в защите программ. А вот когда компьютеры вошли в банковскую сферу и практически в каждый офис, хакерские атаки переориентировались на получение денег или секретной информации. В поле их зрения оказалась аппаратура контроля над космическими аппаратами, ядерными электростанциями, военным комплексом. А ведь успешная атака на такие компьютеры вполне может заменить армию и служить началом «кибервойны».

Арсенал кибервойны - это компьютерные вирусы и черви, меняющие информацию в чужих системах или блокирующие их, а также логические бомбы, троянские кони и программы для компьютерных атак. При этом армейская диспозиция не имеет значения - хакеры могут вести атаку с компьютеров, расположенных в любом городе или даже стране.

Хаос в системах электронных трансакций, службах жизнеобеспечения, не говоря уже о военной сфере, может запросто разрушить колосс на глиняных компьютерных ногах. И эти опасения не напрасны.

Одним из скандалов последних лет прошлого столетия, взбудоражившим всю Америку, стала компьютерная кража военных секретов, якобы совершенная российскими спецслужбами. Конфликт получил название «Лабиринт лунного света» (Moonlight Maze). Американские спецслужбы утверждали, что российские хакеры более года вмешивались в компьютерные сети Министерства обороны и других ведомств, и что в результате этого, возможно, были украдены секретные шифры, используемые ВМФ США, и информация о системах наведения стратегических ракет. Прекращение этих атак вызвало у американцев еще большую панику. Ведь это может означать, что взломщики уже легализовались в их сетях и безнаказанно изучают секретные документы. Пентагон был вынужден издать внутреннее распоряжение, по которому все два миллиона его компьютеров были заблокированы от интернета.

В середине 1999 г. в США специалисты службы безопасности Центра исследования космоса и подводного мира заподозрили, что документы печатаются слишком долго неспроста. Расследование показало, что файлы сначала уходили в один из российских компьютеров и лишь после этого добирались до принтера. Вообще удаленные принтеры - это самая уязвимая часть компьютерной сети офиса. У них есть собственный адрес, и они используют стандартные протоколы, которые легко взломать.

В сфере бизнеса, как мы уже упоминали, все крупные банки используют электронную систему расчетов, при которой клиенты имеют возможность осуществлять денежные переводы со своего счета на другой при помощи персональных компьютеров. Такой облегченный способ расчетов дает неплохой шанс злоумышленникам подключаться к банковским электронным сетям со своего компьютера и использовать деньги клиентов банка.

В принципе обойти все защитные уровни и войти в компьютерную сеть можно, например, подсоединившись к телефонной линии клиента банка, что технически вполне возможно. Записать сеанс общения клиента с банком. Внести в этот сеанс некоторые поправки, а затем через некоторое время запустить его вновь. Деньги пойдут со счета клиента, но, уже с учетом поправок, туда, куда нужно.

Сама акция обычно занимает не более 10 минут. За это время хакер не только успевает проникнуть в компьютерную сеть банка и обойти все ловушки, но и перевести крупные суммы на те самые счета, с которых в заранее обусловленное время сообщники снимают «внезапно» свалившиеся деньги.

Масштабы работы компьютерных мошенников таковы, что в общей сложности каждый день они извлекают со счетов банков и компаний не менее двух миллионов долларов. Преступники, как правило, остаются не наказанными, так как при такой организации дела поймать их практически невозможно. С тех пор, как бизнес многих фирм, работающих в оперативном режиме интернета, пострадал от посторонних атак, осознание опасности изменилось.

Итак, компьютерные атаки совершаются ежедневно, принося даже в мирное время миллиардные убытки. Почему же мы практически ничего про них не слышим? Как показал отчет аудиторской компании Ernst&Yoing, лишь очень немногие «жертвы» обращаются в спецслужбы с просьбой помочь в поисках хакеров. Их удерживает страх потерять доверие клиентов и инвесторов или попасть в суд за утрату конфиденциальной информации.

Диверсионный акт через интернет (то есть уничтожить имеющуюся в базах данных информацию) осуществить гораздо проще, чем изменить программу ЭВМ с целью похищения информации или денежных средств.

Не исключено, что репетицией подобного рода диверсий явились события 7-9 января 2000 г., когда сайты девяти ведущих торговых интернет-компаний подверглись массированному нападению преступников. Общий объем потерь от этой акции составил $1,2 миллиарда. Такой масштабной и одновременно абсолютно бессмысленной интернет-атаки еще не было.

Первым был атакован сайт компании Yahoo!. Утром 7 января на главный сайт компании поступил почти миллиард обращений. Компьютеры оказались не в состоянии справиться с таким количеством информации (число обращений обычно не превышает 200 миллионов в день) и стали выключаться один за другим. Через полчаса сайт Yahoo! отключился от сети. Точно таким же атакам одновременно подверглись сайты других крупнейших торговых и информационных интернет-компаний.

Никаких новых ключей после нападения никто не публиковал. Их просто не было, во всех атаках был использован алгоритм, опубликованный еще в 1999 году немецким хакером по прозвищу Mixter. Схема атаки проста: компьютеры (в этом случае их было около 100), запрограммированные хакером, посылают на сайт-жертву запросы, ничем не отличающиеся от обыкновенных пользовательских, только делают это с огромной частотой. Компьютеры сайта оказываются не в состоянии обрабатывать такое количество запросов и либо выключаются, либо просто сгорают. Особенность такой атаки в том, что ЭВМ не в состоянии отличить ложные запросы от подлинных. То, с чем столкнулась Америка 7-9 января, очень опасно. Здесь атака вообще не предусматривает проникновения в сеть, она просто выводит ее из строя.

**ЗАКЛЮЧЕНИЕ**

Специалисты предупреждают, что в ближайшее время преступления в сфере высоких технологий могут выйти на качественно новый уровень. Нет необходимости захватывать самолет с заложниками. Проще угрожать жизни всех, кто находится в небе, через компьютер, управляющий полетами. Если политический деятель приболел и попал в больницу, вместо «традиционного» покушения на него с помощью винтовки или взрывчатки, проще через интернет взломать защиту локальной сети госпиталя и добраться до системы жизнеобеспечения больного. Небольшое изменение в программе - и результат достигнут. Десятки тысяч людей могут оказаться заложниками, если террорист через сеть вмешается в работу промышленного производства.

Информационные диверсии могут использовать и другие «киберсредства» нападения на компьютерные сети и базы данных, от электронного шпионажа и до вирусов, способных разрушать ключевые системы. К нему относятся программные средства (компьютерные вирусы, программные закладки и пр.), средства радиоэлектронной борьбы, психотропные генераторы и т.д. Следует иметь в виду, что кибердиверсионизм - это не только хакеры или вирусы. Как известно, на большей части компьютеров во всем мире установлена операционная система Windows 95/98/00/ХР/NT, содержимое и внутреннее устройство которой знает лишь очень ограниченный круг лиц на фирме-разработчике. Совершенно не исключено, что эта информация может попасть в руки террористов, которые смогут дать сигнал для переформатирования дисков компьютеров и утери хранящейся на них информации.

В России в настоящее время большая часть (несколько тысяч) коммерческих баз данных функционирует с применением минимальных средств защиты и не обеспечивает необходимого уровня защиты. Все это очень опасно и наносит ощутимый вред как государству в целом, так и конкретным владельцам массивов конфиденциальной информации.

Основой обеспечения эффективной борьбы с кибердиверсионизмом является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению такого рода деятельности. Для борьбы с диверсиями во всех ее проявлениях работают различные антидиверсионные органы. Особое внимание борьбе с диверсиями уделяют развитые страны мира, считая его едва ли не главной опасностью для общества. В России для борьбы с технологическими диверсиями создан специальный орган - Управление «Р», которое занимается борьбой с преступлениями в области высоких технологий. В США с компьютерными нарушителями борются ФБР, ЦРУ, Агентство национальной безопасности, Министерство юстиции, Министерство энергетики, Пентагон и еще десяток различных коммерческих организаций.

Правоохранительные органы России основные надежды в борьбе с компьютерными преступниками возлагают на установку подслушивающих устройств в интернете, с помощью которых можно просматривать сообщения, присылаемые по электронной почте, и отслеживать обращения пользователей к страничкам интернета.

Завершая курсовую работу на тему «Уголовное наказание за диверсии», подчеркнем, что в настоящие время возможности закона в привлечении к уголовной ответственности лиц, причастных к диверсионной деятельности ограничены. Необходимы срочные меры по совершенствованию законодательства в данной сфере.

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ**

1. Конституция Российской Федерации с поправками от 25 июля 2003 г. – СПб, 2003.
2. Уголовный кодекс Российской Федерации с изменениями от 27 июля 2006 – М., 2006.
3. Закон Российской Федерации «О безопасности» // Ведомости Верховного Совета РФ. 2002. № 15; № 2.
4. Ведомости Верховного Совета РСФСР. 1960. № 40
5. Дьяков С.В. Государственные преступления (против основ государственного строя и безопасности государства) и государственная преступность.- М.: Издательство НОРМА, 2003
6. Общенациональная газета «РОССІЯ» №(1)388 10.12.2001
7. Пономарев С.Н. Вступительное слово к теоретическому семинару// Цели уголовного наказания. Рязань, 2004
8. http://www.kavkazcenter.com/russ/sotrud/
1. Террор от лат. terror – страх, ужас. [↑](#footnote-ref-1)
2. Словарь иностранных слов. 10-е изд., стереотип. М. 1983. С. 494. [↑](#footnote-ref-2)
3. http://www.kavkazcenter.com/russ/sotrud/ [↑](#footnote-ref-3)
4. Общенациональная газета «РОССІЯ» №(1)388 10.12.2001

  [↑](#footnote-ref-4)
5. Диверсия от лат. diversio - отклонение, отвлечение. [↑](#footnote-ref-5)
6. Ведомости Верховного Совета РСФСР. 1960. № 40. Ст. 591. [↑](#footnote-ref-6)
7. В ред. Указа Президиума Верховного Совета РСФСР от 30 января 1984 г. и Закона РФ от 18 февраля 1993 г. //Ведомости Верховного Совета РСФСР. 1984. № 5. Ст. 168; Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. № 10. Ст.360. [↑](#footnote-ref-7)
8. См.: Ожегов С.И. Словарь русского языка. – М.: «Русский язык», 2000. [↑](#footnote-ref-8)
9. Дьяков С.В. Государственные преступления (против основ государственного строя и безопасности государства) и государственная преступность.- М.: Издательство НОРМА, 2003, С. 72. [↑](#footnote-ref-9)