## 2.2. Методологические принципы классификации кибероружия

### *2.2.1. Введение в проблему, классификация типов кибероружия*

В соответствующих главах [1, 2] мы детально рассмотрели вопросы терминологии, объекты кибероружия, особенности оборонительного и наступательного кибероружия, в гл. 4 подробно расскажем о вирусах, шпионских «программах», об основных видах информационных атак и приведем конкретные примеры их реализации. В этом вводном разделе мы дадим только общие определения наиболее часто используемых терминов и определений, чтобы читатель был подготовлен к пониманию последующего материала.

Для тех читателей, которые хотят более глубоко изучить все аспекты таких сложных явлений, как киберпреступность, кибероружие, кибербезопасность, мы рекомендуем обратиться к фундаментальной работе *«Понимание киберпреступности: явление, задачи и законодательный ответ»*, которая вышла в свет еще в сентябре 2012 г., но до сих пор является актуальной.

Этот труд был подготовлен специализированным учреждением ООН «International Telecommunication Union – ITU», которое в отечественной литературе называется «Международный союз электросвязи (МСЭ) и в который сегодня входит более 200 стран мира.

Эксперты ООН называют киберпреступность основной угрозой современного общества.

Как показывает ретроспективный анализ истории создания этого ***военно-технического направления*** [1], первыми его использовали различные криминальные группировки (якудза, гангстеры, мафиози и т.п.) для достижения своих криминальных целей без применения классических видов оружия (уничтожение улик в защищенных базах данных, кража денег и конфиденциальной информации и т.д.). По результатам судебных расследований подобных фактов Интерпол поставил в известность об этом новом виде криминальной деятельности спецслужбы развитых государств, которые сразу же оценили не только новые угрозы, но и совершенно новые возможности, которые давало им это оружие.

Если говорить о терминологии этого нового вида оружия – информационно-технического, то иногда это оружие называют одной из разновидностей «кибероружия», а иногда – «информационного оружия».

Наверное, наиболее близким к сути проблемы являются определения и классификации, изложенные в открытых руководящих документах вооруженных сил (ВС) США в области информационного противоборства (да, такие подразделения официально существуют в США уже много лет!), где это современное оружие называется «кибернетическим» и разделяется на две большие группы: ***информационно-психологическое*** и ***информационно-техническое*** [1, 2].

Главными объектами первого вида этого кибероружия являются люди, а второго – технические объекты (программное и аппаратное обеспечение).

Как известно из открытых источников информации, в США, Китае и в странах НАТО уже много лет активно разрабатываются различные концепции войн XXII века, где кибероружию отдается основополагающая роль.

Здесь имеется в виду использование разработанных в «закрытых» институтах и лабораториях специальных средств, под воздействием которых происходят заданные изменения в информационных и социальных системах противника. В соответствии с этой концепцией применять это оружие планируется на трех уровнях одновременно: на стратегическом, тактическом и оперативном. Основными объектами его воздействия прежде всего являются информационно-технические (информационно-коммутационные, телекоммуникационные и т.п.) системы, все существующие сегодня социальные системы, инфраструктурные объекты (энергетика, транспорт, управление воздушным движением) отдельные группы лиц и даже отдельные личности (криминальные «авторитеты», «авторитетные» политики и высшие военные чины).

Пока наиболее широко (по сравнению с кибероружием) в открытой печати освещено только состояние разработки психофизического оружия (зарубежные военные называют его нейронным оружием). Психофизическое оружие – совокупность различных методов и средств (технотронных, психотропных, суггестивных, когнитивных и пр.) скрытого насильственного воздействия на подсознание человека в целях нужной заказчику модификации (изменения) подсознания (и в итоге – сознания человека), его поведения и психического состояния в интересах воздействующей стороны (государства, группы лиц или отдельного «сверхчеловека»), хотя психофизическое оружие (нейронное оружие) по сути представляет собой всего лишь одну из многочисленных разновидностей кибероружия. В следующей главе мы подробно рассмотрим все особенности этого опаснейшего вида оружия.

***Информационно-техническому (кибернетическому) оружию присущи принципиально важные качественные характеристики, отличающие его от всех других известных видов оружия и дающие ему несомненные преимущества:*** *универсальность*, *скрытность*, *высокую техническую эффективность*, *экономическую эффективность*, возможность применения для решения задач как ***стратегического***, так и ***тактического*** и ***оперативного*** уровней, *невозможность организации эффективного и достоверного международного контроля* за созданием (разработкой) и испытаниями этого оружия, принципиальную возможность организации так называемого *эффекта кролика*, когда воздействие только на один элемент информационного ресурса атакуемого объекта может привести к лавинной реакции вплоть до отказа всей информационной или управляющей системы потенциального противника.

В фундаментальной работе Ричарда Пойсела (Richard A. Poisel) «Iformation and Electronic warfare» детально рассмотрены теоретические и методологические основы, математические модели, а также конкретные технические решения основных видов информационного оружия (Information warfare – IW) и так называемого электронного оружия (Electronic warfare – EW).

Информационное оружие и информационное воздействие (Information operations – IO) здесь рассматриваются как новый подход к ведению современных войн с использованием информационных технологий (Informstion technologies – IT), а именно как следующий эволюционный этап стратегии ведения боевых действий (warfighting). ***Только тот, кто имеет больше информации и умеет лучше и быстрее ее обрабатывать, сможет победить в современной войне***. По принятой на Западе

терминологии современное информационное оружие подразделяется на пять основных видов (категорий):

– электронное оружие (Electronic Warefare – EW);
– операции в компьютерных сетях (computer network operations – CNO);
– психологическое оружие (psychological operations – PSY OPS);
– «военная хитрость» (military deception – MILDEC);
– секретные операции (operation security – OPSEC).

CNO-оружие предназначено для атак (как активных, так и пассивных) различных компьютерных, информационных и телекоммуникационных сетей, включая мобильные сети связи.

PSYORS-оружие предназначено для воздействия на сознание гражданского населения, причем не только населения страны «противника», но и собственного населения.

EW-оружие включает в себя все аспекты построения электронных систем, которые используют электромагнитное излучение в различных целях.

Во всем мире все больше промышленных и социальных систем управляются с помощью компьютерных сетей (например, концепция «умный город»): это электроснабжение, отопление, канализация, управление транспортными потоками и т.д.

Понятно, что успешная кибератака нанесет «защищающейся стороне» не меньший урон, чем применение ядерного оружия: отключение важных инфраструктурных объектов мгновенно введет в хаос крупные мегаполисы и целые регионы.

Авторитетные эксперты утверждают, что на момент выхода этой книги наиболее профессионально подготовленные и многочисленные «кибервойска» имеет правительство США. Так, например, агентство Zecurion Analytics приводит такие цифры:

Общий бюджет американских «кибервойск» в 2017 году превысил 7 млрд долл., а их численность – 9 тысяч «киберсолдат». Уже в 2018 году их численность, вероятно, превысит 10 тысяч человек, поскольку руководитель управления кибербезопасности АНБ Пол Наканса на одном из брифингов заявил СМИ о принятом решении создать новое специализированное подразделение по борьбе с онлайн-угрозами со стороны российских хакеров.

Второе место в этом «рейтинге» эксперты отдают КНР: 20 тысяч «киберсолдат» с ежегодным бюджетом 1,5 млрд долл.

Великобритания на этом фоне выглядит достаточно скромно: она содержит чуть более 2 тысяч хакеров с бюджетом 450 млн долл.

Экспертные оценки по КНДР расходятся: от 700 до 6000 хакеров с бюджетом от 400 до 900 млн долл.

В этом списке Россия занимает скромное место – не более 1000 специалистов при годовом бюджете 300 млн долл. Косвенно эти данные подтверждают и российские СМИ. Так, еще в январе 2017 года министр обороны РФ С. Шойгу официально подтвердил факт создания в составе МО РФ специальных киберподразделений.

О наличии таких действующих киберподразделений свидетельствует и тот факт, что еще в 2013 году во время проведения белорусско-российских учений «Запад-2013» одним из таких подразделений «условного агрессора» была смоделирована ситуация масштабной кибератаки на информационные и управляющие ресурсы «защищающейся стороны». Другое подразделение при этом «успешно

отразило учебную кибератаку, максимально приближенную к реальным боевым условиям».

Что касается Беларуси, известно, что МО РБ в том же 2013 году объявило набор гражданских специалистов в сфере IT, а в начале 2018 года началось создание специальной IT-роты, укомплектованной специалистами белорусского Парка высоких технологий.

В свою очередь, ***отдельные составные компоненты кибероружия подразделяются на следующие группы: оборонительные, атакующие и комбинированные***.

Следует отметить, что такие защитные средства, как криптографическая защита, антивирусная защита, средства обнаружения (предотвращения) несанкционированных вторжений (атак), ранее рассматривались только в качестве одного из важных элементов обеспечения информационной безопасности и противодействия несанкционированному доступу со стороны некоторых нарушителей (хакеров).

В отечественной технической литературе и в нормативных документах по проблемам информационной безопасности часто встречаются такие термины, как *«**доверенная** операционная система», «**доверенная** среда», «**доверенный** канал», «**доверенная** связь», «модуль **доверенной** полезной нагрузки»* и т.д.

В то же время вы нигде не найдете четких определений термина ***«доверенный»***.

Обычно под *доверенной системой* отечественные специалисты по безопасности понимают ***систему, использующую аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.***

Фактически это является ***аналогом английского термина «Trusted computer system»***, который был введен еще в 1985 г. американским нормативным документом «Department of defense trusted computer system evalution criteria».

Мы сочли целесообразным привести здесь максимально близко к тексту оригинала также и классификацию, предложенную еще в 2013 г. в работе «Проблемы классификации кибероружия» (В.В. Каберник, «Вестник МГИМО») [3]. По нашему мнению, это одна из немногих работ в области ***именно научной*** классификации кибероружия, поскольку оперирует понятиями из области кибернетики. Автор формализовал так называемые признаки кибероружия, разделив все типы кибероружия на четыре типа:

– избирательные системы;
– адаптивные системы с внешним управлением;
– автономные адаптивные системы;
– автономные самообучающиеся системы.

Основные особенности ***первого типа*** характеризуются следующими чертами.

1. Воздействие на систему является информационным, отсутствует физическое вмешательство.
2. Воздействие происходит на строго определенную систему или на тип систем с эксплуатацией их уязвимостей.
3. Результатом воздействия является предсказуемый и повторяемый результат.
4. Воздействие необязательно «разрушительно», целью является прежде всего нарушение нормального функционирования.

Автор вводит и некоторые «уточняющие» признаки для этого типа кибероружия, а именно:

1. Воздействие кибероружия происходит ***внутри*** ограниченных систем.
2. Целью кибероружия являются системы и комплексы, действующие по *однозначно установленным законам и алгоритмам*.

С этими уточнениями комплекс классификационных признаков кибероружия приобретает необходимую сфокусированность. Обратим внимание на то, что под описанные признаки попадают не только программотехнические системы, но и любые автоматы, функционирующие по известным законам. Казалось бы, этим автор избыточно расширяет спектр рассматриваемых систем. Тем не менее такое расширение является обоснованным.

Автор [3] сравнивает два примера: в *одном* целью воздействия абстрактного кибероружия является программный комплекс управления атомным реактором, *не подключенный* к исполнительным устройствам, например, тестовый стенд; в другом целью воздействия является такой же комплекс, *управляющий* действующим реактором. Результатом нарушения функционирования этого комплекса в первом случае будут сравнительно безобидные программные сбои.

Во *втором* же случае результаты будут существенно изменяться в зависимости от схемы управления и способов функционирования подключенных к системе исполнительных устройств. Как известно, в хорошо спроектированной отказоустойчивой системе программные сбои могут эффективно парироваться на уровне оконечных управляемых автоматов, которые имеют свои дополнительные (например, чисто механические) подсистемы обеспечения безопасности. Поэтому для целенаправленного воздействия (кибератаки) при его планировании необходимо также учитывать особенности работы этих конечных автоматов, возможные способы отключения предохранительных систем, изъяны конструкции, дефекты проектирования и т.п.

Из приведенного выше сравнения следует вывод о том, что ***для создания кибероружия первого типа необходимо глубокое знание и понимание способов функционирования объекта воздействия (системы)***. Исследование уязвимостей только программного кода может оказаться недостаточным: нарушение функционирования управляющей программы необязательно приведет к фатальным сбоям. Восстановление системы при отсутствии фатальных повреждений в этом случае может быть достигнуто простой переустановкой программного обеспечения.

Еще более устойчивы *распределенные* системы, где необходимый уровень нарушения функционирования может быть достигнут только согласованным *воздействием на несколько подсистем одновременно*.

Отметим еще одну особенность. Кибероружие первого типа эксплуатирует известные уязвимости системы, которые могут быть устранены ее разработчиками при наличии информации о самом факте существования такого оружия. Нет сомнений, что эти уязвимости будут устранены в обязательном порядке при зарегистрированном факте применения оружия.

Таким образом, кибероружие первого типа имеет практическую ценность только в том случае, если *обеспечена секретность его разработки*; сокрыт факт его наличия и внезапность его применения. Иными словами, кибероружие первого типа явля-

ется едва ли не *одноразовым*. Если факт его использования или сам факт наличия известен противнику, он приложит все усилия для ликвидации уязвимостей систем, которые являются целью этого оружия. Такая характеристика позволяет говорить о том, что кибероружие первого типа чаще всего является *наступательным*, ориентированным на нанесение эффективного первого удара.

Примером кибероружия первого типа является ныне широко известный компьютерный червь Stuxnet. Обратим внимание на то, что его целью являлась совершенно конкретная система с известными уязвимостями, в том числе и на уровне конечных исполнительных устройств. Воздействие крайне избирательно: червь практически безвреден для других систем, используя их только как *способ доставки* к заданной цели.

Но попробуем рассмотреть и некоторые следствия прецедента Stuxnet. Исследование уязвимостей цели воздействия не могло не требовать глубокого знания принципов ее функционирования. Из этого следует, что создание данного конкретного образца вредоносного ПО стало возможным только благодаря масштабной разведывательной операции одновременно с нарушением основных принципов построения системы безопасности на объекте, который стал целью воздействия. Сам же образец Stuxnet является в этом контексте лишь вершиной айсберга: специальным средством, разработанным в *единичном экземпляре и использованным однократно* для осуществления конкретной диверсии. Иными словами, Stuxnet следует сравнивать с заказными разработками разведывательного сообщества; это оружие никогда *не предназначалось для массового использования*. Такие черты не могут быть признаны характерными для всех возможных образцов кибероружия первого типа, но их следует признать довольно типичными.

Высокая стоимость разработки и предварительных НИОКР, однократность применения, беспрецедентная избирательность поражения и необходимость обеспечения секретности разработки и доставки делают подобные образцы кибероружия непрактичными для реального *войскового применения*. Они переходят в разряд *специальных средств* арсенала спецслужб. Кроме того, отдельные образцы (существование которых с высокой долей вероятности можно предположить, хотя оно никак не разглашается в открытых источниках) кибероружия первого типа могут быть использованы для нейтрализации критической инфраструктуры противника в целях повышения эффективности первого удара либо ослабления способностей противника противостоять ему. *Фактически это те же диверсионные операции*, предшествующие началу полномасштабных боевых действий.

Интересно отметить, что способы массированного применения таких образцов сходны со структурой *первого обезоруживающего ядерного удара,* что в некоторых вариантах рассмотрения позволяет причислить такие (описанные абстрактно) разработки к *стратегическим наступательным вооружениям*.

***Ко второму типу*** относятся адаптивные системы с внешним управлением. Выделенный выше признак № 2 характерен для несложных автономных систем. Запрограммированность действий не позволяет применять их против целей, которые значительно отличаются по структуре построения подсистем безопасности. В то же время, если мы рассматриваем модульную систему, этот признак необязательно должен выполняться. Абстрактно *такой комплекс кибероружия может быть описан*

*как информационная система, состоящая из четырех блоков: проникновения; сбора информации; связи и управления; модернизации*. Схема воздействия такого кибероружия на целевую систему описывается в следующей последовательности.

1. Используя модуль проникновения, вредоносная часть оружия внедряется в систему.
2. Используя модуль связи и управления, червь предоставляет операторам дополнительную информацию.
3. Пользуясь полученной информацией, операторы выбирают оптимальные способы воздействия на эту конкретную цель.
4. Используя модуль мутации, вредоносное ПО модифицирует себя, приобретая новые свойства.

В описанной последовательности пункты 3 и 4 могут повторяться произвольное число раз. Таким образом, внутри целевой системы червь может проходить последовательную модернизацию, эффективно обходя вновь возникающие способы защиты. Описанная модульная система, очевидно, нацелена прежде всего на выполнение *задач шпионажа* на длительном отрезке времени. Однако принципы, использованные в ее построении, пригодны также для создания долгоживущей «закладки» в информационной системе противника. В то время как шпионский вариант такого оружия может выдать себя как минимум регулярно отсылаемой информацией, адаптивная «закладка» после проникновения в целевую систему может вообще не выдавать себя. Более того, пользуясь своей системой мутаций, она способна, к примеру, избавиться от ненужного уже модуля проникновения, который нередко является характерным признаком, по которому производится поиск вредоносного ПО. Применение адаптивных систем с внешним управлением в разведывательных целях наблюдалось для червей Flame и комплекса Red October.

Тем не менее второму типу кибероружия присущ *существенный недостаток: потребность в действующем канале связи*. Это не только позволяет обнаружить присутствие «закладок», но и резко снижает ценность такой системы для проведения атак на цели, изолированные от общедоступных связных каналов (например, не имеющие выхода в Интернет, что характерно для практически всех армейских систем). Поэтому перспективы использования адаптивных систем с внешним управлением в качестве кибероружия ограничены.

Но при этом нельзя не отметить важное преимущество систем второго типа: сравнительно низкую стоимость разработки такого оружия. В отличие от автономных систем, система с внешним управлением требует для своей разработки вложений лишь в эффективный модуль проникновения и отчасти в модуль мутаций. Дополнительные вредоносные модули могут разрабатываться и внедряться по мере необходимости. Показательно то, что кибероружие второго типа наиболее часто ассоциируется с китайскими разработками, в то время как США и другие страны Запада больше полагаются на сложные и дорогостоящие автономные системы.

***Третий тип***: автономная адаптивная система. Для определенных классов целей возможно создание *полностью автономной адаптивной системы*, которая, опираясь на базу знаний об уязвимостях целевой системы, сможет самостоятельно выбирать оптимальный вариант воздействия (кибератаки). Очевидно, что спектр таких вариантов будет ограничен и уровень адаптивности оружия третьего типа тоже

уступает системам второго типа. Но при этом появляется важнейшее *преимущество: независимость от связи с оператором*. Кибероружие третьего типа уже начинает в высокой степени соответствовать требованиям к классическому оружию поля боя: не предъявляет высоких требований к квалификации оператора, сравнительно просто в применении необученным персоналом, процедура применения может быть предельно автоматизирована.

*Кибероружие третьего типа, по сути, является экспертной системой*, опирающейся на базу знаний об объекте воздействия, накопленную разведывательными службами классическими методами. В этом его сходство с оружием первого типа, и из этого следует, что создание кибероружия третьего типа также сопряжено со значительными затратами. От оружия второго типа третий тип наследует только модульную схему построения, позволяющую комбинировать различные способы воздействия на целевую систему и при необходимости способность изменять себя в зависимости от внешних факторов. Но при этом кибероружие третьего типа является завершенным комплексом и фактически является уже полноценным оружием поля боя, но крайне дорогостоящим. Его распространение и совершенствование пока остается практичным лишь в отдельных узких нишах высокотехнологичной войны.

***Четвертый тип:*** автономная самообучающаяся система. Автор работы [3] полагает, что этот четвертый тип кибероружия пока существует лишь как *умозрительная конструкция*. Абстрактно его можно описать как систему искусственного интеллекта, которая способна произвольным образом модифицировать себя для автономного проникновения в целевую систему, ее анализа и последующего *самостоятельного* выбора оптимального способа воздействия.

Фактически такая абстрактная система является развитием вышеописанных второго и третьего типов, но не нуждается ни в операторе, ни в экспертной системе, поскольку способна вырабатывать решения самостоятельно. Как полагает и сам автор приведенной классификации, с учетом довольно скромного прогресса в развитии систем искусственного интеллекта и высоких рисков разработки в среднесрочной перспективе действующих образцов кибероружия четвертого типа создано не будет. Для разработчиков кибероружия еще довольно долго будет перспективнее совершенствовать системы третьего типа. Дополнительным сдерживающим фактором, ограничивающим разработку систем четвертого типа, является крайне узкая ниша их использования и *непредсказуемое поведение* автономной самообучающейся системы.

Известно, что правительствами всех развитых индустриальных стран наложено негласное вето на публикации в открытой периодической научно-технической печати ключевых технических моментов, касающихся концепций и перспектив дальнейшего развития этого научно-технического направления, что, в частности, можно объяснить ведущейся передовыми мировыми державами информационной войной Востока и Запада («белый порошок» в Ираке, «дела» Березовского, Литвиненко, Скрипаля, «вмешательство русских» в президентские выборы США, не существующие в реальности химические атаки в Сирии и т.д.).

Под это *вето* попали и технические аспекты развития наиболее эффективных методов противодействия киберугрозам. В то же время военные ведомства миро-

вых держав-лидеров, прекрасно понимая реальное положение дел и возможные уникальные перспективы развития этого направления, финансируют в достаточно больших объемах целый ряд как отдельных проектов, так и специальных комплексных программ.

Для достижения поставленных целей в арсеналах разведывательных сообществ имеются многочисленные технические и программные средства, разнообразные «аксессуары» для организации скрытых технических каналов утечки секретной информации, не последнее значение здесь имеет так называемый человеческий фактор или использование различных видов «внедренных» и «добровольных» агентов (недоброжелателей).

### *2.2.2. Виды информационных атак*

Итак, существует два основных способа повлиять на информационные функции противника – косвенно или напрямую. Проиллюстрируем разницу между ними на примере. Пусть наша цель – заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам. Косвенная информационная атака реализуется следующим образом: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения и имитировать деятельность по работе с ними. Мы полагаемся на то, что противник будет визуально наблюдать ложный аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник, по нашему мнению. Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться.

Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же нужное нам решение – производить переброску войск через другие коммуникации.

### *2.2.3. Способы внедрения в состав информационных ресурсов противника вредоносных программ*

Бурное развитие электронной техники и ее все более глубокое проникновение во все сферы жизни, включая государственное и военное управление, обусловили появление в последнее время принципиально нового вида противоборства государств – информационного («информационной войны»).

Под термином *«информационная война»* понимается комплекс мероприятий, направленных на предотвращение несанкционированного использования, повреждения или уничтожения элементов собственной информационной инфраструктуры (ИИ), а также использование, нарушение целостности или уничтожение элементов

ИИ противника в целях обеспечения информационного превосходства в мирное время, а также на различных этапах подготовки и ведения боевых действий.

Для ведения информационной войны разрабатываются специфические средства, которые могут быть оборонительными и наступательными.

Потребность в создании именно многоуровневой системы защиты связана с тем, что взаимосвязь всех перспективных информационных систем предполагается осуществить через средства единой для пользователей любого уровня глобальной коммуникационной сети. Разрабатываемые средства (сетевые шифраторы, комплект программных технических средств) должны будут обеспечивать проверку законности доступа к информационным ресурсам, идентификацию пользователей, регистрацию всех действий потребителей и персонала с возможностью оперативного и последующего анализа, а также необходимый уровень конфиденциальности.

По способам внедрения в состав информационных ресурсов противника и воздействия на них наступательные средства программно-технического воздействия (СПТВ) подразделяются на следующие классы:

- «логическая бомба» – скрытая управляющая программа, которая по определенному сигналу или в установленное время приходит в действие, уничтожая или искажая информацию, воспрещая доступ к тем или иным важным фрагментам управляющего информационного ресурса или дезорганизуя работу технических средств. Подобное вмешательство в АСУ войсками и оружием может коренным образом повлиять на ход и исход боя, операции;
- «программный вирус» – специализированный программный продукт, способный воспроизводить логические бомбы и внедрять их дистанционно в информационные сети противника, самостоятельно размножаться, прикрепляться к программам, передаваться по сети;
- «троянский конь» – программа, внедрение которой позволяет осуществить скрытый несанкционированный доступ к информационному массиву противника для добывания разведывательной информации;
- нейтрализатор тестовых программ, обеспечивающий сохранение естественных и искусственных недостатков программного обеспечения (ПО);
- преднамеренно созданные, скрытые от обычного пользователя интерфейсы для входа в систему, вводимые в ПО разработчиками с корыстными или диверсионно-подрывными целями;
- малогабаритные устройства, способные генерировать ЭМИ высокой мощности, обеспечивающий вывод из строя радиоэлектронной аппаратуры.

В качестве первоочередных объектов применения СПТВ с точки зрения нанесения максимально возможного ущерба могут рассматриваться информационные элементы систем предупреждения о ракетном нападении и контроля космического пространства, пунктов управления высшего звена и обслуживающих их вычислительных центров и узлов связи. В мирное время подобного рода воздействие может оказываться на такие важные для государства цели, как банковская система, система управления воздушным движением, системы управления гидроэлектростанциями также может оказываться психологическое воздействие на население государства-противника с помощью средств радио- и телевизионного вещания.

К характерным чертам СПТВ можно отнести универсальность, скрытность, внезапность, экономичность, многовариантность и свободу пространственно-временного маневра.

### *2.2.4. Классификация основных видов кибервоздействий*

Надо сказать, что до сих пор не существует устоявшейся общепризнанной терминологии и классификации в сфере информационного (кибернетического) оружия, что в некоторой степени связано с соображениями секретности, проблемами национальной безопасности, проблемами «большого бизнеса» и др.

В англоязычной печати различным аспектам проблемы информационного оружия посвящено множество работ. Здесь следует привести только наиболее цитируемые:

- Richard A. Poisel. Information Warfare and Electronic Warfare Systems. – Artech House, 2013. – 414 p.;
- Antonimos A. Tsirigotis. Cybernetics, warfare and Discourse: The Cybernetisation of Warfare in Britain. – Palgrave Macmillan, 2017;
- Clay Wilson. Information Operadions, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues. – CRS Report for Congress. Order Code RL 31787. – March 20. – 2007.

Наиболее близкими к сути проблемы являются определения и классификации, изложенные в открытых руководящих документах вооруженных сил (ВС) США в области информационного противоборства [1, 8], где современное информационное (кибернетическое) оружие разделяется на две большие группы: информационно-психологическое и информационно-техническое.

Главными объектами первого вида информационного оружия (кибероружия) являются люди, второго – техника (программное и аппаратное обеспечение).

Как известно из ряда открытых источников, в США, Китае, России и в странах НАТО активно разрабатываются различные концепции войн XXII века, где кибероружию (информационному оружию – ИО) отводится основополагающая роль.

Здесь ИО – использование специально разработанных в «закрытых» институтах и лабораториях специальных средств, под воздействием которых происходят заданные изменения в информационных и социальных системах. В соответствии с этой концепцией применять ИО планируется на трех уровнях одновременно: на стратегическом, тактическом и оперативном. Основными объектами его воздействия прежде всего являются информационно-технические (информационно-коммутационные, телекоммуникационные и т.п.) системы, социальные системы, группы лиц и даже отдельные личности (групповое и индивидуальное сознание, говоря языком политтехнологов). Наиболее широко (по сравнению с кибероружием) в открытой печати освящено состояние разработки психофизического и нейронного оружия. Психофизическое оружие – совокупность различных методов и средств (технотронных, психотропных, суггестивных, когнитивных и пр.) скрытого насильственного воздействия на подсознание человека в целях нужной заказчику модификации (изменения) подсознания (и в итоге сознания человека), поведения и психического состояния в интересах воздействующей стороны (госу-

дарства, группы лиц или отдельного «сверхчеловека»). Психофизическое оружие представляет собой всего лишь одну из многочисленных разновидностей информационно-психологического оружия [9, 18, 19].

Если говорить о терминологии, то наиболее общим, по мнению авторов [7], является следующее: *«Информационное оружие – это различные средства информационного воздействия на технику и людей в целях решения задач воздействующей стороны»*.

Информационному (кибернетическому) оружию также присущи некоторые важные качественные характеристики, отличающие его от всех других известных видов оружия:

- универсальность: его применение не зависит от климатических и географических условий, сезонов года, времени суток и т.п.;
- скрытность: для его применения не требуется создавать и применять большие группировки военной техники и живой силы;
- техническая эффективность: хотя его действие визуально невозможно достоверно зафиксировать (документировать), результаты его воздействия на атакуемую сторону сопоставимы с воздействием оружия массового поражения;
- экономическая эффективность: его разработка, механизмы подготовки и применение требуют существенно меньших затрат по сравнению с другими видами оружия;
- возможность применения для решения задач как стратегического, так и тактического и оперативного уровней;
- невозможность организации эффективного и достоверного контроля за созданием (разработкой) и испытаниями информационного оружия. На момент выхода этой книги официально не установлено ни одного документально подтвержденного факта его применения;
- возможность организации так называемого эффекта кролика, когда воздействие только на один элемент информационного ресурса может привести к лавинной реакции вплоть до отказа всей информационной или управляющей системы.

И еще один момент надо принять во внимание: ***темпы совершенствования любого вида атакующего оружия на всей обозримой истории его развития всегда опережали темпы развития технологий защиты и противодействия ему, и информационное оружие, конечно же, не является исключением из правил***.

По целевому назначению информационное оружие подразделяют на две большие группы [8, 20]: оборонительное и наступательное.

*Наступательное* информационное оружие решает задачи воздействия на систему принятия решений противника путем скрытого поражения наиболее критичных ее компонентов.

*Оборонительное* информационное оружие решает задачи обороны в многоуровневой информационной войне и включает в себя системы многоуровневой информационной безопасности и соответствующего противодействия.

Отличительной особенностью ИО является его ориентированность на скрытое поражение программных и аппаратных средств систем передачи, обработки и

хранения различных данных, функционирующих в сфере информационного пространства или в киберпространстве.

Основные задачи наступательного НИО:

– целенаправленное изменение (искажение, уничтожение, копирование) или блокирование информации;
– преодоление систем защиты, создаваемых средствами оборонительного информационного оружия;
– осуществление технической дезинформации;
– нарушение по заданному алгоритму нормального функционирования информационно-коммуникационных систем (телекоммуникационных, навигационных, метеорологических, связных, систем защиты оборонных и военных государственных объектов, атомных станций, нефте- и газотранспортных систем и др.).

Для выполнения этих основных задач НИО должно обладать комплексом аппаратных и программных средств, отслеживающих несанкционированный доступ к любым базам данных, нарушения известного режима функционирования атакуемых программно-аппаратных средств вплоть до мгновенного полного вывода из строя ключевых элементов информационно-управляющей инфраструктуры отдельного государства и даже группы союзных государств.

В свою очередь, отдельные составные компоненты НИО подразделяются на группы [9]: обеспечивающие, атакующие и комбинированные; следует отметить, что ранее средства оборонительных (защитных) информационно-технических воздействий не рассматривались специалистами именно в качестве одной из компонент защиты от кибероружия – в качестве оборонительного ИТО. А именно такие защитные средства, как криптографическая защита, антивирусная защита, средства обнаружения-предотвращения несанкционированных вторжений (атак), рассматривались только как один из важных элементов обеспечения информационной безопасности и противодействия несанкционированному доступу со стороны некоторых нарушителей (хакеров).

Однако в условиях реально ведущихся кибератак, когда имеет место информационное противоборство в технической сфере, по мнению российских экспертов [7], необходимо ввести классификационную категорию «оборонительное информационно-техническое оружие» (ОИТО).

Наиболее точная классификация современного информационно-технического оружия представлена на рис 2.3.

Так, например, по этой классификации обеспечивающее информационно-техническое оружие применяется для сбора данных, обеспечивающих эффективное применение оборонительного или атакующего информационно-технического (и другого) оружия, а также против стандартных средств защиты атакуемой системы [9].

Обеспечивающее ИО включает в себя следующие компоненты:

1) средства разведки:
   – традиционные средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
   – средства компьютерной разведки (как программные, так и доступа к физической инфраструктуре);
   – средства ведения разведки на основе открытых источников;

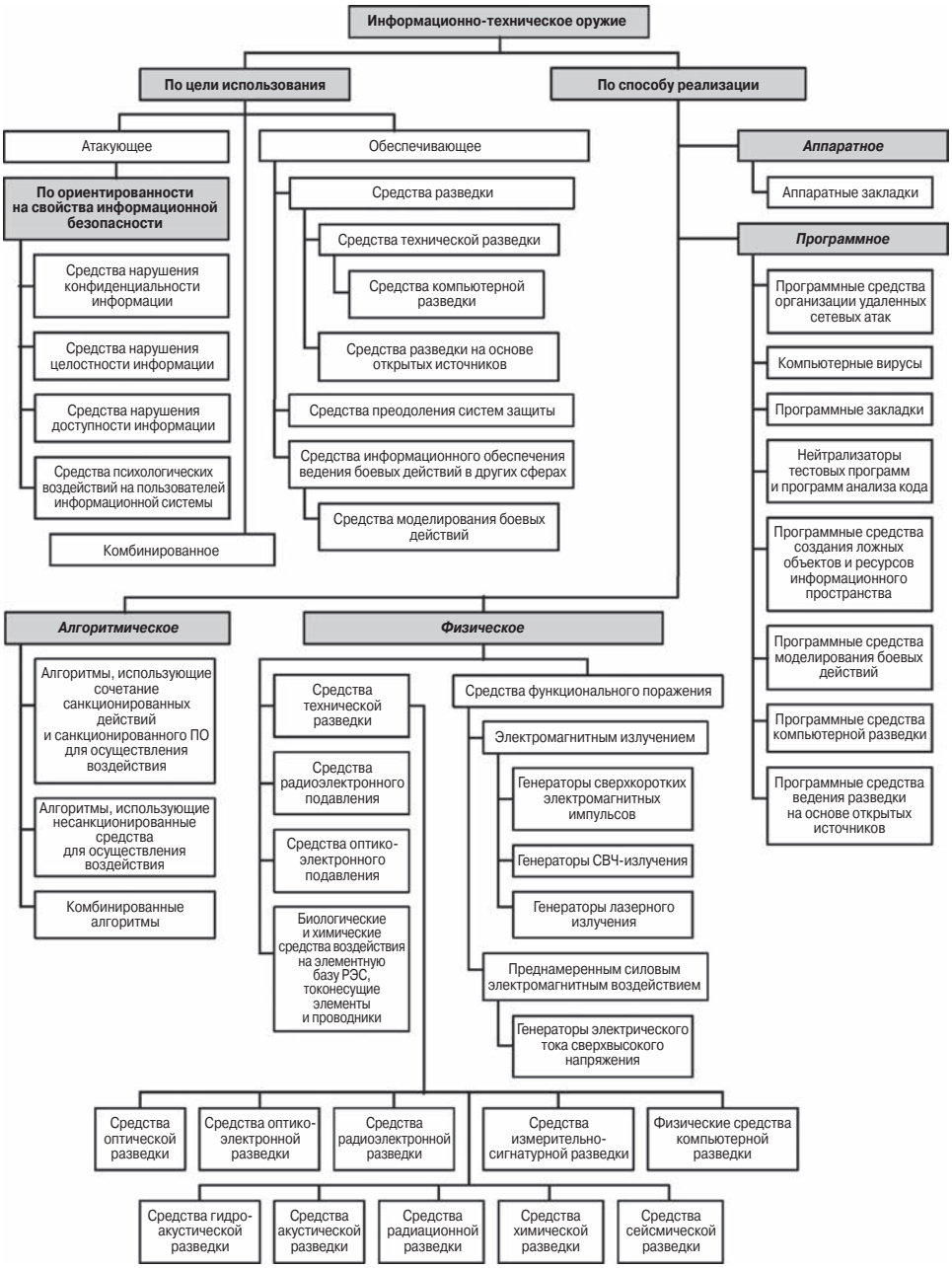


**Рис. 2.3.** Классификация информационно-технического оружия [8]

2) специальные средства преодоления систем защиты;

3) средства информационного обеспечения процесса ведения боевых действий в других сферах.

Средства разведки, как правило, выступают в качестве обеспечивающего оружия. Они позволяют получить информацию об атакующих средствах инфор-

мационного оружия противника и способах его применения, что позволяет более рационально сконфигурировать собственные средства информационно-технической защиты. Воздействие средств разведки проявляется как в виде пассивных действий, направленных на добывание информации и, как правило, связанных с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

Успешное применение средств преодоления систем защиты позволяет осуществлять эффективные воздействия на хранимую, обрабатываемую и передаваемую в системе информацию с использованием атакующего информационно-технического оружия.

Хотя это не относится к последующему материалу книги, отдельно стоит выделить средства информационного обеспечения ведения боевых действий в других сферах. Под такими средствами понимаются не автоматизированные системы управления и различного рода комплексы автоматизации, а широко используемые военными всего мира комплексы для моделирования боевых действий, которые позволяют путем многократного прогона модели найти оптимальный состав сил и средств, а также оптимальную стратегию их действий при любом вероятном сценарии действий противника.

Атакующее информационное оружие – это оружие, с помощью которого осуществляется воздействие на хранимую, обрабатываемую и передаваемую в системе информацию, нарушающее используемые в системе информационные технологии [9].

Атакующее информационное оружие, в свою очередь, можно разделить на четыре основных вида [9]:

– средства нарушения конфиденциальности информации;
– средства нарушения целостности информации;
– средства нарушения доступности информации;
– средства психологического воздействия на пользователей информационной системы.

Применение атакующего информационного оружия направлено на срыв выполнения информационной системой целевых задач.

Как правило, атакующее информационное оружие включает в себя следующие компоненты, объединенные в единую систему [26]:

– средства доставки оружия;
– средства преодоления подсистемы защиты атакуемой системы;
– полезную нагрузку.

По способу реализации информационное оружие можно разделить на следующие классы [9, 14]:

– алгоритмическое;
– программное;
– аппаратное;
– физическое.

Информационное оружие, относящееся к разным классам, может применяться совместно.

К алгоритмическому информационному оружию относятся [9]:

– алгоритмы, использующие сочетание санкционированных действий и санкционированного (легального) программного обеспечения для осуществления в итоге несанкционированного воздействия на информационные ресурсы;
– алгоритмы использования несанкционированных средств (другого информационно-технического оружия – программного, аппаратного, физического) для осуществления несанкционированного воздействия на информационные ресурсы;
– комбинированные алгоритмы, состоящие из различных алгоритмов предыдущих двух типов.

Разновидностью алгоритмического оружия являются *эксплойт* (exploit) – потенциально невредоносный набор данных (например, санкционированная последовательность команд, графический файл или сетевой пакет нестандартного размера, запрос на установление соединения), который некорректно обрабатывается информационной системой, работающей с такими данными, вследствие ошибок в ней. Результатом некорректной обработки такого набора данных может быть перевод информационной системы в уязвимое состояние.

Типовым примером алгоритмического оружия является DoS-атака (Denial of Service – отказ в обслуживании), заключающаяся в том, что на атакуемую систему с высокой интенсивностью посылаются вполне корректные запросы на использование ее информационных ресурсов. Это ведет к тому, что возможности информационной системы по обслуживанию таких запросов быстро исчерпываются и в итоге она отказывает в обслуживании всем своим пользователям.

К *программному* ИТО относят программное обеспечение для проведения атак на информационные системы противника:

– программные закладки;
– программные средства организации удаленных сетевых атак;
– компьютерные вирусы;
– нейтрализаторы тестовых программ и программ анализа кода.

Программные средства обеспечивающих задач в традиционных сферах применения оружия (воздух, земля, море):

– программные средства создания ложных объектов и ресурсов информационного пространства (виртуальные машины);
– программные средства моделирования боевых действий;
– программные средства компьютерной разведки.

К *аппаратному* информационному оружию (АИО) относят аппаратные средства, которые изначально встроены в информационную систему (или несанкционированно внедренные в нее), а также санкционированные аппаратные средства, обладающие недекларируемыми возможностями, которые позволяют в процессе своей работы производить несанкционированное воздействие на информационные ресурсы системы. К наиболее распространенному типу аппаратного информационно-технического оружия относятся аппаратные закладки (аппаратные трояны).

К *физическому* ИТО относятся средства добывания информации путем доступа к «физической» инфраструктуре атакуемого информационного пространства, анализу генерируемых этой инфраструктурой различных физических полей, а также

средства радиоэлектронного и, конечно, хорошо понятного военным огневого поражения ее физических элементов, хотя более корректным следует считать отнесение к физическому информационно-техническому оружию только тех средств, которые предназначены исключительно для воздействия на технические элементы информационной системы.

По мнению авторов, наиболее полно классификацию физического информационно-технического оружия можно представить в соответствии с работами [1, 14, 20]:

- средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации и внедрение закладок;
- средства радиоэлектронного подавления (РЭП);
- средства оптико-электронного подавления;
- средства функционального поражения электромагнитным излучением (ЭМИ) – генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения и др.;
- биологические и химические средства воздействия на элементную базу радиоэлектронных систем (РЭС), их токонесущие элементы и проводники (например, графитовые бомбы).

### *2.2.5. Классификация основных видов кибервоздействий*

Информационно-техническое воздействие (ИТВ) – основной поражающий фактор информационного оружия, представляющий собой воздействие либо на информационный ресурс, либо на информационную систему, либо на средства получения, передачи, обработки, хранения и воспроизведения информации в ее составе с целью вызвать заданные структурные и/или функциональные изменения.

Объекты информационного воздействия – информация, ее свойства, связанные с информационной безопасностью, информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.), технические средства, компьютерные системы и информационно-вычислительные сети, а также другая инфраструктура высокотехнологического обеспечения жизни общества и функционирования системы управления государством, вооружением и военной техникой.

На рис. 2.4 представлена детализированная классификация известных информационных воздействий, предложенная авторами фундаментальной работы [7]. Различают следующие виды информационных воздействий:

- одиночные;
- групповые.

Информационные воздействия также классифицируют по характеру поражающих свойств [9, 17]:

- высокоточные воздействия (например, на определенный ресурс в информационно-вычислительной сети);
- комплексные воздействия (например, вся информационно-телекоммуникационная инфраструктура).

По типу воздействий на информацию или информационный ресурс информационные воздействия могут быть:

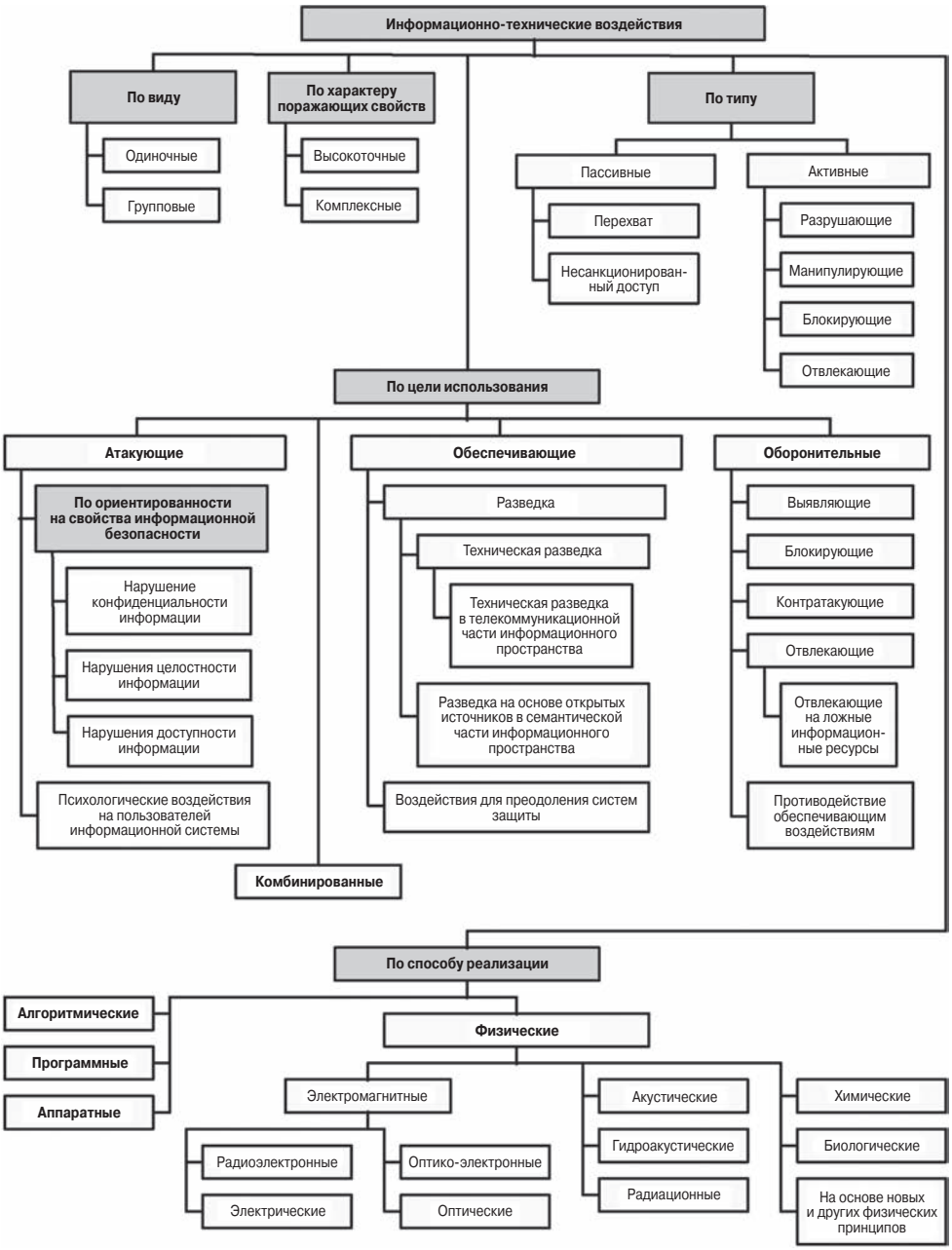


**Рис. 2.4.** Классификация информационных воздействий [8]

– пассивными (перехват, несанкционированный доступ);
– активными (разрушающие воздействия, манипулирующие воздействия, блокирующие воздействия).

Пассивные воздействия не оказывают непосредственного влияния на работу атакуемой информационной системы, но могут нарушать ее политику безопас-

ности. Именно отсутствие непосредственного влияния на функционирование информационной системы приводит к тому, что пассивное воздействие очень трудно обнаружить. Примером пассивного воздействия является (широко используемая спецслужбами) разведка параметров информационных систем.

Активное воздействие оказывает непосредственное влияние на функционирование атакуемой информационной системы (изменение конфигурации системы, нарушение работоспособности и т.д.) и нарушает принятую в ней политику безопасности. Важной особенностью активного воздействия, в отличие от пассивного, является принципиальная возможность его обнаружения, так как в результате его осуществления в информационной системе происходят определенные деструктивные изменения, которые можно оперативно выявить.

По цели использования информационные воздействия могут быть классифицированы на:

– обеспечивающие;
– атакующие;
– оборонительные;
– комбинированные.

По способу реализации информационные воздействия могут быть разделены на:

– алгоритмические;
– программные;
– аппаратные;
– физические.

В частности, к последним относятся следующие:

– электромагнитные (среди них отдельно можно выделить воздействия на основе различных электромагнитных волн: СВЧ-оружие, радиоэлектронные, оптико-электронные, оптические, электрические);
– акустические;
– гидроакустические;
– радиационные;
– химические;
– биологические;
– на основе новых и других физических принципов.

Классификация информационных воздействий в общем случае по смыслу совпадает с классификацией информационного оружия, за исключением оборонительных воздействий. Ранее средства оборонительных информационных воздействий не рассматривались в качестве оборонительного информационного оружия, вместе с тем они реально существуют и играют одну из ведущих ролей в информационном противоборстве при организации защиты собственной стороны.

Основной целью использования оборонительных информационных воздействий является организация эффективного противодействия информационному оружию противника. Их можно классифицировать следующим образом (рис. 2.4)

– *выявляющие* – это воздействия, ориентированные на выявление как самого факта, так и последовательности атакующих воздействий противника;
– *блокирующие* – воздействия, ориентированные на блокировку как выявленных, так и потенциальных атакующих воздействий противника;

– *контратакующие* – воздействия на информацию, информационные ресурсы и информационную инфраструктуру противника в целях срыва его атакующих воздействий;
– *отвлекающие* – воздействия, ориентированные на дезинформацию противника, отвлечение его атакующих или обеспечивающих воздействий на незначащие или ложные объекты;
– *противодействие обеспечивающим воздействиям противника* – это способы маскировки, обеспечения безопасности, повышения скрытности реальных режимов функционирования, а также способы мониторинга реальных возможных каналов утечки в отношении собственных информационных систем.

Самое короткое определение средств информационного воздействия: это различные средства, используемые в качестве информационного оружия или для защиты от него [9].

Необходимо отметить, что классификация атакующих и обеспечивающих информационных воздействий в общем виде совпадает с классификацией соответствующих видов информационного оружия. Однако необходимость защиты от атакующих и обеспечивающих информационных воздействий противника вынуждает дополнительно выделить так называемые оборонительные средства информационного воздействия, к которым можно отнести [8]:

– средства технического анализа элементной базы РЭС для выявления аппаратных закладок (троянов) и недекларируемых возможностей;
– системы обнаружения и предотвращения вторжений;
– средства антивирусной защиты;
– средства криптографической защиты;
– средства создания ложных объектов и ресурсов в защищаемом информационном пространстве.

Применительно к новейшим разработкам атакующего информационного оружия наибольшее развитие получили средства специального программно-математического воздействия, которые объединяют возможности алгоритмического и программного информационного оружия.

Средства специального программно-математического воздействия – это обычно комплекс программ, способных выполнить любое подмножество перечисленных ниже основных функций [9, 27]:

– скрывать признаки своего присутствия в программно-аппаратной среде информационной системы;
– разрушать (искажать) код программ в памяти информационной системы;
– обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
– подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию, передаваемую по каналам управления;
– сохранять фрагменты информации из памяти информационной системы в некоторой области внешней памяти прямого доступа (локальной и удаленной);

– искажать, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных;
– противодействовать работе тестовых программ и систем защиты информационных ресурсов.

К основным средствам информационного воздействия, классифицированным *по способу реализации,* можно отнести:

1) алгоритмические средства воздействия (атакующие):
   – эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйверы, BIOS);
   – эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования (например, вирус Stuxnet, внедренный в АСУ технологическим процессом обогащения урана, за счет перехвата и модификации команд);
   – эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
   – эксплойты, ориентированные на сетевые протоколы информационной системы;
2) программные средства воздействия:
   – атакующие:
     • компьютерные вирусы;
     • программные закладки;
     • нейтрализаторы тестовых программ и программ анализа кода;
   – обеспечивающие:
     • программные средства для моделирования боевых действий;
     • программные средства компьютерной разведки в телекоммуникационной части информационного пространства;
   – оборонительные средства воздействия:
     • программные средства антивирусной защиты;
     • системы обнаружения и предотвращения вторжений;
     • программные средства криптографической защиты;
     • средства тестирования программного обеспечения и анализа кода для выявления программных закладок и недекларируемых возможностей;
     • средства создания ложных объектов и ресурсов в информационном пространстве;
3) аппаратные средства воздействия:
   – атакующие (аппаратные закладки);
   – оборонительные – средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;
4) физические средства воздействия:
   – атакующие средства:
   – средства радиоэлектронного противодействия;

– средства оптико-электронного подавления;
– средства функционального поражения электромагнитным излучением (генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения);
– средства и комплексы функционального поражения преднамеренными силовыми электромагнитными воздействиями (генераторы электрического тока сверхвысокого напряжения);
– биологические и химические средства воздействия на элементную базу радиоэлектронных систем, токонесущие элементы и проводники (например, графитовые бомбы);
– обеспечивающие средства:
– средства технической разведки (в том числе и средства компьютерной разведки).

Здесь необходимо отметить, что к средствам технической разведки, представленным в данной классификации, относятся те средства, которые добывают информацию об атакующих средствах информационного оружия противника и способах его применения, т.е. фактически они являются средствами обеспечивающего информационного оружия. Средства технической разведки сами могут оказывать воздействие на объекты противника как путем пассивных действий, направленных на добывание информации, так и путем активных действий (атак), направленных на создание условий, благоприятствующих добыванию информации.

Схема классификации основных средств информационных воздействий представлена на рис. 2.5 [8].

Рассмотрим более подробно принцип работы наиболее распространенных из представленных на рис. 2.5 средств информационного воздействия. Ввиду того что антивирусные средства защиты, системы обнаружения и предотвращения вторжений, а также криптографические и стеганографические средства защиты довольно подробно рассмотрены в известной литературе (например, в работе [28]), здесь основное внимание уделим только следующим наиболее распространенным информационным воздействиям и средствам их проведения:

– удаленные сетевые атаки;
– компьютерные вирусы;
– программные закладки;
– аппаратные закладки;
– нейтрализаторы тестовых программ и программ анализа кода;
– средства создания ложных объектов информационного пространства;
– средства технической разведки.

Интересна история создания и первого внедрения Stuxnet. Эта совместная операция американских и израильских спецслужб носила кодовое название «Олимпийские игры» и проводилась поэтапно в период с 2007 по 2013 г. Целью операции было вывести из строя иранское производство по обогащению урана. Рассматривались различные варианты решения этой задачи, включая возможность применения ракетой атаки и бомбового удара, но в итоге было принято решение о проведении спецоперации с использованием элементов информационного оружия (кибероружия).

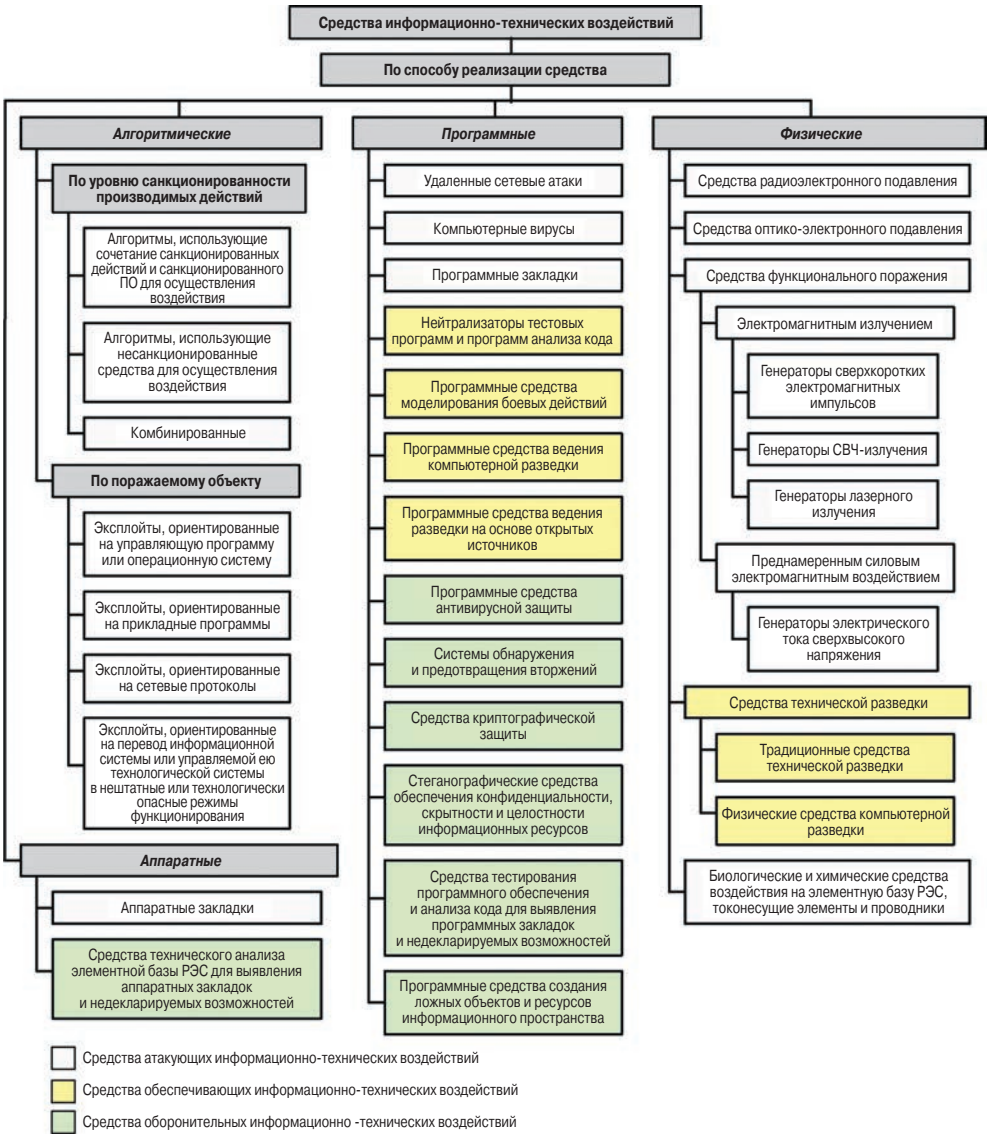


**Рис. 2.5.** Классификация средств информационного воздействия [8]

Вот так в кратком изложении выглядят основные этапы (технические аспекты) создания и проведения кибератаки на иранский завод по обогащению урана в г. Натанзе [1].

1. Совместными усилиями программистов из АНБ и израильской разведки (подразделение 8200) в 2007 году было создано вредоносное программное обеспечение (первая версия компьютерного червя – разновидность программного обеспечения, самостоятельно распространяющегося в локальных и глобальных компьютерных сетях под названием Stuxnet), предназначенное для выведения из строя технологического оборудования (в данном случае центрифуг) на производстве по обогащению урана.

Разработка продолжалась в течение восьми месяцев.

Этот червь должен был внедрить в специализированные компьютеры (промышленные контроллеры), которые управляли центрифугами, вредоносный код и при этом длительное время себя никоим образом не обнаружить. В определенный момент внесенная вредоносная программа начинала активизироваться, заставляя центрифуги чрезмерно ускоряться или резко тормозиться, что приводило к их поломке.

При этом на пульте оператора центрифуг все было нормально (штатно).

2. Внедрение вредоносной программы в заводскую локальную сеть управления производственным процессом, которая была изолирована от глобальной компьютерной сети (Интернета), осуществлялось в два этапа.

Вначале с помощью завербованного агента (иранского технического специалиста), имевшего доступ к заводским компьютерам, первая версия компьютерного червя посредством прямого подключения флешки к компьютеру, связанному с внутренней компьютерной сетью управления производственным циклом, переселилась во внутреннюю архитектуру незащищенных контроллеров фирмы «Сименс», которые непосредственно управляли конкретными центрифугами. Затем немецкие инженеры, которые обслуживали эти контроллеры, в обновленном программном обеспечении, не зная про внедренный в это обеспечение компьютерный червь, невольно предоставили разработчикам из АНБ и израильской разведки данные о практических результатах внедрения первой версии червя в локальную сеть иранского завода.

Затем на основе этой информации специалисты АНБ и израильской разведки доработали первую версию червя Stuxnet, используя широко распространенные контроллеры фирмы «Сименс», аналогичные используемым для управления иранскими центрифугами. Опробование доработанной версии на образцах центрифуг, идентичных используемым иранцами, прошло успешно. Таким же образом с помощью агента новая версия червя Stuxnet была внедрена на иранский завод в г. Натанзе. Когда пришла пора действовать, червь Stuxnet начал ретранслировать записанные сигналы на пульты, с которых операторы управляли центрифугами, что приводило к разгону их до немыслимых скоростей, резкому торможению их вращения и выходу центрифуг из строя. Эта кибератака имела несколько активных фаз, которые разделяли случайные интервалы времени, что привело к поломке большого количества центрифуг.

3. Иранские специалисты для устранения возникающих аварийных ситуаций, которые они связали с плохим качеством центрифуг, провели замену части обслуживающего персонала и полную замену оборудования на заводе по обогащению урана в г. Натанзе, оснастив его моделями центрифуг нового поколения. Но и для них американцы с израильтянами разработали новую версию червя Stuxnet, которая была внедрена в ноутбук иранского физика-ядерщика и впоследствии через подключение к компьютерной сети завода переселилась в контроллеры, управляющие центрифугами. При этом когда иранец позже подключил свой ноутбук к сети Интернет, этот червь Stuxnet новейшей модификации «вырвался на свободу» и начал плодить свои копии в других компьютерах по всему миру. И когда находил в компьютерной сети контроллеры фирмы «Сименс», переходил в активное состояние и осуществлял кибердиверсии.

В дальнейшем в течение 2010–2013 годов этот червь заразил в различных странах множество компьютеров, использующих операционную систему WINDOWS, пока совместными усилиями компьютерных экспертов не была ограничена его активность.

### *2.2.6. Удаленные сетевые атаки как наиболее распространенные типы кибервоздействий*

С учетом определения и классификации удаленных воздействий на распределенные вычислительные системы, представленные в работах [8, 29], можно дать следующее определение этому виду воздействия.

*Удаленная сетевая атака* – это разрушающее или дестабилизирующее информационное воздействие, осуществляемое по каналам связи удаленным относительно атакуемой системы субъектом и характерное для структурно- и пространственно-распределенных информационных систем.

Удаленные сетевые атаки становятся возможными благодаря наличию «уязвимостей» в существующих протоколах обмена данными и в подсистемах защиты распределенных информационных систем. При этом к основным известным «уязвимостям» информационных систем, которые позволяют проводить против них успешные удаленные сетевые атаки, относятся [28, 29]:

- несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации эксплойтов и ошибок в программном обеспечении;
- открытость информационной системы, свободный доступ к информации по организации сетевого взаимодействия, способам защиты, применяемым в системе;
- наличие ошибок в операционных системах, прикладном программном обеспечении, протоколах сетевого обмена;
- разнородность используемых версий программного обеспечения и операционных систем;
- ошибки конфигурирования систем и средств защиты;
- «экономия» на средствах и системах обеспечения безопасности (или игнорирование их).

В соответствии с различными основаниями удаленные сетевые атаки можно классифицировать следующим образом (рис. 2.6) [1].

1. По характеру воздействия все атаки можно разделить на две категории [28, 29]:
   - пассивное воздействие;
   - активное воздействие.

Пассивное воздействие не оказывает непосредственного «видимого» влияния на работу информационной системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование атакуемой системы приводит к тому, что пассивную сетевую атаку практически невозможно обнаружить. Типовым примером такой пассивной удаленной сетевой атаки является прослушивание канала связи.

Активное воздействие оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, наруше-

ние работоспособности и т.д.) и нарушает принятую в ней политику безопасности.

Практически все известные типы удаленных сетевых атак относятся к активным воздействиям. Очевидной особенностью активного воздействия, по сравнению с пассивным, является принципиальная возможность его обнаружения, так как в результате его осуществления в информационной системе происходят определенные деструктивные изменения.

2. По воздействию на свойства информационной безопасности [28, 29]:
   - перехват информации – нарушение конфиденциальности информационных ресурсов системы;
   - искажение информации – нарушение целостности информационных ресурсов системы;
   - нарушение работоспособности системы – нарушение доступности информационных ресурсов.

Перехват информации означает получение к ней доступа, но при этом обычно возможность ее модификации отсутствует. Следовательно, перехват информации ведет к нарушению ее конфиденциальности: осуществляется несанкционированный доступ к информации без возможности ее искажения. Также очевидно, что нарушение конфиденциальности информации является пассивной сетевой атакой. Примером такой атаки, связанной с перехватом информации, может служить просмотр (прослушивание) канала в сети.

Искажение информации означает либо полный контроль над информационным потоком между объектами распределенной системы, либо возможность передачи сообщений от имени другого объекта, в любом случае подобное искажение информации ведет к нарушению целостности информационных ресурсов системы. Примером такой удаленной сетевой атаки, целью которой является нарушение целостности информационных ресурсов, может служить атака, связанная с внедрением ложного сетевого объекта в систему, например внедрение ложного DNS-сервера.

При нарушении работоспособности системы атакующей стороной обычно не планируется получение несанкционированного доступа к информации. Ее основная цель – добиться, чтобы элементы распределенной информационной системы на атакуемом объекте вышли из строя, а для всех остальных объектов системы доступ к информационным ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить DoS-атака.

3. По условию начала осуществления воздействия [28, 29]:
   - атака по запросу от атакуемого объекта;
   - атака по наступлению ожидаемого события на атакуемом объекте;
   - безусловная атака.

При атаке по запросу от атакуемого объекта атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов могут служить DNS- и ARP-запросы. Важно отметить, что данный тип удаленных атак наиболее характерен для распределенных сетевых информационных систем.

При атаке по условию наступления ожидаемого события атакующий осуществляет наблюдение за состоянием информационной системы, которая является целью атаки. При возникновении определенного события в этой системе атакующий немедленно начинает воздействие на нее. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сама атакуемая система. Такие сетевые атаки довольно распространены. Примером такой атаки может быть атака, связанная с несанкционированным доступом к информационным ресурсам компьютера по сети после факта его успешного заражения backdoor – вирусом, который создает дополнительные «уязвимости» в подсистеме защиты компьютера.

При безусловной атаке она осуществляется немедленно и безотносительно к состоянию информационной системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

4. По наличию обратной связи с атакуемым объектом [28, 29]:
   – с обратной связью;
   – без обратной связи (однонаправленная атака).

Удаленная сетевая атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ. Следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адаптивно реагировать на все изменения, происходящие на атакуемом объекте. Подобные удаленные атаки наиболее характерны для распределенных сетевых информационных систем.

В отличие от атак с обратной связью удаленным сетевым атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных команд, ответы на которые атакующему не нужны. Подобную сетевую атаку можно называть однонаправленной удаленной атакой. Примером такой однонаправленной атаки может служить DoS-атака.

5. По расположению субъекта атаки относительно атакуемого объекта [28, 29] различают два случая:
   – внутрисетевая атака;
   – межсетевая атака.

В случае внутрисетевой атаки субъект и объект атаки находятся в одной сети. При межсетевой атаке субъект и объект атаки находятся в разных сетях.

Важно отметить, что межсетевая удаленная атака представляет гораздо большую опасность, чем внутрисетевая. Это связано с тем, что в случае межсетевой атаки ее объект и непосредственно атакующий могут находиться на значительном расстоянии друг от друга, что может существенно воспрепятствовать эффективным мерам по отражению атаки.

6. По уровню эталонной модели OSI, на котором осуществляется воздействие [28, 29]:
   – физический;
   – канальный;
   – сетевой;

– транспортный;
– сеансовый;
– представительный;
– прикладной.

Удаленные атаки обычно ориентированы на сетевые протоколы, функционирующие на различных уровнях модели OSI. При этом надо отметить, что атаки, ориентированные на физический, канальный, сетевой и транспортный уровни, как правило, направлены против сетевой инфраструктуры – оборудования узлов сети и каналов связи. Атаки, ориентированные на сеансовый, представительный и прикладной уровни, как правило, направлены против оконечных терминалов сети. В связи с этим в зависимости от уровня OSI, на который ориентирована атака, конкретный вид используемого воздействия может значительно меняться. Это может быть воздействие средств РЭП или ЭМИ при атаке, ориентированной на физический уровень, при этом эффекты от такого воздействия отображаются на более верхних уровнях модели OSI. Это может быть и DoS-атака на узловое оборудование сети, и вирус, поражающий операционную систему конечного терминального оборудования.

### *2.2.7. Примеры реализации кибервоздействий с использованием метода удаленных сетевых атак*

В связи с тем что удаленные сетевые атаки совместно с воздействием вирусных средств составляют подавляющее большинство всех информационных воздействий, рассмотрим их более подробно.

К основным способам и средствам информационного воздействия, которые можно классифицировать как удаленные сетевые атаки, относятся (рис. 2.7) [28, 29]:

– анализ сетевого трафика;
– подмена доверенного объекта или субъекта информационной системы;
– внедрение ложного объекта в информационную систему:
– внедрение ложного объекта путем навязывания ложного сетевого маршрута;
– внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети;
– путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
– путем формирования потока ложных ответов не дожидаясь запросов от узлов сети;
– использование ложного сетевого объекта для организации удаленной атаки на информационную систему:
– селекция информации и сохранение ее на ложном сетевом объекте;
– модификация информации, проходящей через ложный сетевой объект;
– подмена информации, проходящей через ложный сетевой объект;
– атаки типа «отказ в обслуживании» подразделяются на следующие виды:
– отказ в обслуживании (DoS-атака);
– распределенная атака «отказ в обслуживании» (DDoS-атака);
– зацикливание процедуры обработки запроса.