

УДК 004.7: 623.618

Информационное оружие в технической сфере: терминология, классификация, примеры

Макаренко С. И.

Актуальность. Адекватное описание противоборства в информационной сфере требует формирования соответствующего терминологического базиса. Одним из основных элементов этого базиса является понятие «информационное оружие». При этом теория информационного оружия в психологической сфере, а также его применение для влияния на социально-политические процессы достаточно глубоко разработана в имеющихся работах. Однако терминологический аппарат в области понятий и классификации информационного оружия в технической сфере отличается противоречивостью и неоднозначностью. В связи с этим уточнение терминологии в области информационно-технического оружия и проведение его системной классификации является актуальной задачей. **Целью работы** является уточнение терминологического базиса в области информационного оружия в технической сфере, а также введение его строгой классификации. **Новизной работы** является авторский подход к системе терминов, определений и классификации информационно-технического оружия и информационно-технических воздействий, основанный на методах системного анализа и логического обобщения известных работ. Также к элементам новизны стоит отнести выявленные частные тенденции развития наиболее распространенных средств информационно-технического воздействия. **Практическая значимость.** Представленный анализ может быть использован техническими специалистами для обоснования новых технологических решений в области информационной безопасности, а также военными специалистами – для обоснования новых форм и способов информационного противоборства. Кроме того, данный анализ будет полезен научным работникам и соискателям, ведущим научные и диссертационные исследования для прикладного обоснования целесообразности предлагаемых ими улучшений безопасности информационных систем.

Ключевые слова: информационное противоборство, информационное оружие, информационно-техническое оружие, информационно-техническое воздействие, удаленные сетевые атаки, сетевые атаки, вирусы, программные закладки, аппаратные закладки, нейтрализаторы тестовых программ, ложные объекты информационного пространства, средства моделирования боевых действий, средства технической разведки, средства разведки по открытым источникам, Большие Данные.

Введение

Адекватное описание противоборства в информационной сфере потребовало формирования соответствующего терминологического базиса. В США и странах НАТО еще с 90-х годов введены руководящие документы, определяющие терминологию и, зачастую, именно ей руководствуются исследователи в области информационного противоборства. Обзор этой терминологии представлен в более ранней работе автора [1]. Вместе с тем за пределами анализа, выполненного в этой работе, осталось понятие информационного оружия. При этом теория информационного оружия в психологической сфере и его применение для влияния на социально-политические процессы достаточно широко представлена в работах таких специалистов как: И.Н. Панарин, Г.Г. Почепцов, А.В. Манойло, С.П. Расторгуев, С.Г. Кара-Мурза, В.В. Цыганов, С.Н. Бухарин, Д.А. Новиков, А.Г. Чхартишвили, а также других ученых. Однако терминологический аппарат

в области понятий и классификации информационного оружия в технической сфере отличается противоречивостью и неоднозначностью. В качестве примера можно привести работы С.Н. Гриняева [2], А.В. Бедрицкого [3], В.К. Новикова [4], С.А. Петренко [5], Л.В. Воронцовой, Д.Б. Фролова [6], Н.П. Шеховцеова, Ю.Е. Кулешова [7], Е.Д. Паршаковой [8]. Представленные в этих работах варианты классификации информационного оружия в технической сфере и информационно-технических воздействий не обладают высокой степенью систематизации, и зачастую ведутся без учета методов системного подхода. К наиболее систематизированному изложению понятий информационного оружия можно отнести словарь [9]. Однако, представленные в этом словаре понятия не объединены к строгой классификационной системе.

В связи с вышеуказанным, в статье предлагается авторский подход к системе терминов, определений и классификации информационно-технического оружия и информационно-технических воздействий. В основу статьи положены материалы открытых источников, а именно – анализ руководящих документов Вооруженных сил (ВС) США в области информационного противоборства [1], дополненный материалом публикаций отечественных специалистов в данной предметной области.

Структурно статья состоит из трех разделов:

- 1) информационное оружие – анализ терминологии, а также его классификация;
- 2) информационно-техническое оружие – анализ терминологии; определения информационно-технического оружия и информационно-технических воздействий, а также их классификация;
- 3) наиболее распространенные средства информационно-технического воздействия – анализ способов и примеров применения, определений и квалификация для наиболее распространенных средств:
 - удаленных сетевых атак;
 - вирусов;
 - программных закладок;
 - аппаратных закладок;
 - нейтрализаторов тестовых программ;
 - ложных объектов информационного пространства;
 - средств моделирования боевых и военных действий;
 - средств технической разведки;
 - средств компьютерной разведки;
 - средств разведки по открытым источникам.

1. Информационное оружие

1.1 Определение информационного оружия

В настоящее время нередко к информационному оружию относят широкий класс приемов и способов информационного воздействия на противника – от дезинформации и пропаганды до средств радиоэлектронной борьбы. При этом на сегодняшний день нет единого толкования понятия

«информационное оружие». В различных источниках приводятся различные определения этого понятия. При этом наиболее общим является следующее.

Информационное оружие – совокупность средств информационного воздействия на технику и людей [2, 10].

В соответствии со сферами, в которых ведется информационное противоборство, информационное оружие подразделяется на два основных вида [2, 10]:

- 1) информационно-техническое оружие;
- 2) информационно-психологическое (также включает в себя психофизическое оружие).

Главными объектами информационного оружия первого вида является техника, второго – люди.

Психофизическое оружие – это совокупность всех возможных методов и средств (технотронных, суггестивных, психотропных, комплексных и др.) скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении. Психофизическое оружие представляет собой разновидность информационно-психологического оружия [2, 11].

Фактически информационное оружие является технологией, включающей в себя [2, 12]:

- анализ способов и механизмов активизации у конкретной информационной системы противника, свойственных ей программ самоуничтожения, деградации или дестабилизации;
- поиск такой программы;
- разработка конкретного информационного оружия;
- применение информационного оружия по заданному объекту.

Полковник ВВС США Р. Сафрански, один из идеологов концепции сетецентрической войны, дает достаточно широкое определение информационному оружию.

Информационное оружие – использование специально подобранных средств, под воздействием которых происходит изменение процессов в информационных и в социальных системах в соответствии с поставленными целями [13]. В соответствии с разработанной Р. Сафрански концепцией, применять информационное оружие предполагается на стратегическом, оперативном и тактическом уровнях. При этом основными объектами его воздействия являются информационно-технические системы, социальные системы, отдельные личности или группы лиц (то есть групповое и индивидуальное сознание) [13].

Оригинальный подход к определению понятия «информационное оружие» сделан в работе [14]. В соответствии с этой работой дано следующее определение.

Информационное оружие – различные средства поражения: высокоточное оружие для поражения органов управления или отдельных радиоэлектронных средств, средства радиоэлектронной борьбы, источники

мощного электромагнитного импульса, программные вирусы и др., эффективно решающие задачи информационной войны [14].

Спорным в данном подходе является отнесение к классу информационного оружия большинства средств поражения и физического оружия по той лишь причине, что оно обеспечивает физическое уничтожение органов управления и радиоэлектронных систем (РЭС) противника.

В работах [15] и [16] приводятся близкие по смыслу определения информационного оружия.

Информационное оружие – совокупность информационных технологий, способов и средств информационного воздействия, предназначенных для ведения информационной войны [15].

Информационное оружие – оружие, наиболее эффективно решающее задачи информационной войны, основной задачей которой является достижение информационного превосходства [16].

Указывая на недостаток двух приведенных выше определений информационного оружия, заключающийся в привязке данного понятия к неоднозначно трактуемому в различных источниках понятию «информационная война», автор монографии [11] приводит следующее определение этого вида оружия.

Информационное оружие – это средства информационного воздействия на технику и людей с целью решения задач воздействующей стороны, и специфичные способы их применения [11].

Это определение, а также определение, представленное в работах [2, 10], на взгляд автора являются наиболее общими и полными и включают в себя всю совокупность средств для организации воздействий, которые могут быть использованы для деструктивного влияния как в технической, так и в психологической сфере.

В работе [13] авторами сделана другая попытка обобщения и конкретизации вышеуказанных определений информационного оружия.

Информационное оружие – это совокупность способов и средств [13]:

- подавления элементов инфраструктуры государственного и военного управления противника;
- электромагнитного влияния на элементы информационных и телекоммуникационных систем;
- несанкционированного доступа к информационным ресурсам с последующей их деформацией, уничтожением или хищением;
- информационно-психологического воздействия на военнослужащих и гражданское население противоборствующей стороны.

Информационному оружию присущи следующие качественные характеристики, которыми оно отличается от других видов оружия [17]:

- универсальность – его применение не зависит от климатических и географических условий, времени суток, сезонов года и т.п.;
- скрытость – для его применения не требуется проводить мобилизацию, создавать большие группировки войск, в то же время его действие

- незаметно, а по воздействию сопоставимо с оружием массового поражения;
- внезапность применения – не требуется его длительная подготовка;
 - экономическая эффективность – разработка информационного оружия и его применение требует существенно меньших затрат по сравнению с другими видами оружия;
 - масштабность применения как для решения задач стратегического, так и тактического уровня;
 - эффект «цепной реакции» – воздействие информационного оружия на отдельный элемент информационной системы информационного ресурса может привести к выводу из строя других элементов системы, а затем и системы в целом;
 - сложность осуществления контроля за созданием и испытанием информационного оружия – его разработку, а в ряде случаев и сам факт применения можно надежно скрыть от разведки противника.

При этом темпы совершенствования информационного оружия (как, впрочем, и любого вида атакующего вооружения) превышают темпы развития технологий защиты и противодействия ему [2].

1.2 Общая классификация информационного оружия

В соответствии со сферой своего применения информационное оружие подразделяется на [13]:

- информационно-техническое оружие;
- информационно-психологическое оружие.

В соответствии со своим целевым назначением информационное оружие подразделяется на два типа [13]:

- оборонительное информационное оружие;
- наступательное информационное оружие.

Оборонительное информационное оружие решает задачи обороны в информационной войне и включает системы многоуровневой информационной безопасности и различные системы противодействия информационно-психологическому оружию противника. Таким образом, в состав оборонительной составляющей информационного оружия входят средства противодействия и нейтрализации наступательного информационного оружия противника [13].

Наступательное информационное оружие решает задачи воздействия на систему принятия решения противника путем поражения наиболее критичных ее компонентов (как в технической, так и психологической сферах) [13].

2. Информационно-техническое оружие

2.1 Определение и классификация информационно-технического оружия

Особенностью информационно-технического оружия является его ориентированность на поражение аппаратно-программных средств систем передачи, хранения и обработки информации, функционирующих в технической сфере информационного пространства (в киберпространстве).

Взяв за основу определения информационного оружия, ориентированного на применение в технической сфере, представленные в работах [2, 7, 18], можно дать следующее определение.

Информационно-техническое оружие – совокупность специально организованной информации, информационных технологий, способов и средств, позволяющих целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование систем обработки информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, а также другой инфраструктуры высокотехнологического обеспечения жизни общества и функционирования системы управления государством, применяемое в ходе информационной операции для достижения поставленных целей.

В соответствии с этим определением информационно-техническое оружие включает технические и программные средства, обеспечивающие несанкционированный доступ к базам данных, нарушение штатного режима функционирования аппаратно-программных средств, а также вывод из строя ключевых элементов информационной инфраструктуры отдельного государства или группы государств.

В соответствии с различными основаниями, информационно-техническое оружие можно классифицировать следующим образом (рис. 1).

1. По цели использования информационно-техническое оружие делят на [2]:

- обеспечивающее;
- атакующее;
- комбинированное.

Рассматривая данную классификацию, надо отметить, что традиционно, средства оборонительных информационно-технических воздействий не рассматриваются в качестве оборонительного информационно-технического оружия. В настоящее время сложился подход, в котором оборонительные средства (средства антивирусной защиты, системы обнаружения и предотвращения вторжений, средства криптографической защиты и т.д.) рассматриваются как элемент обеспечения информационной безопасности и противодействия несанкционированному доступу со стороны некоторых отдельных нарушителей. Вместе с тем в условиях, когда будет вестись информационное противоборство в технической сфере, такой подход может

вызвать путаницу в определениях, и потребует введения категории «оборонительное информационно-техническое оружие».

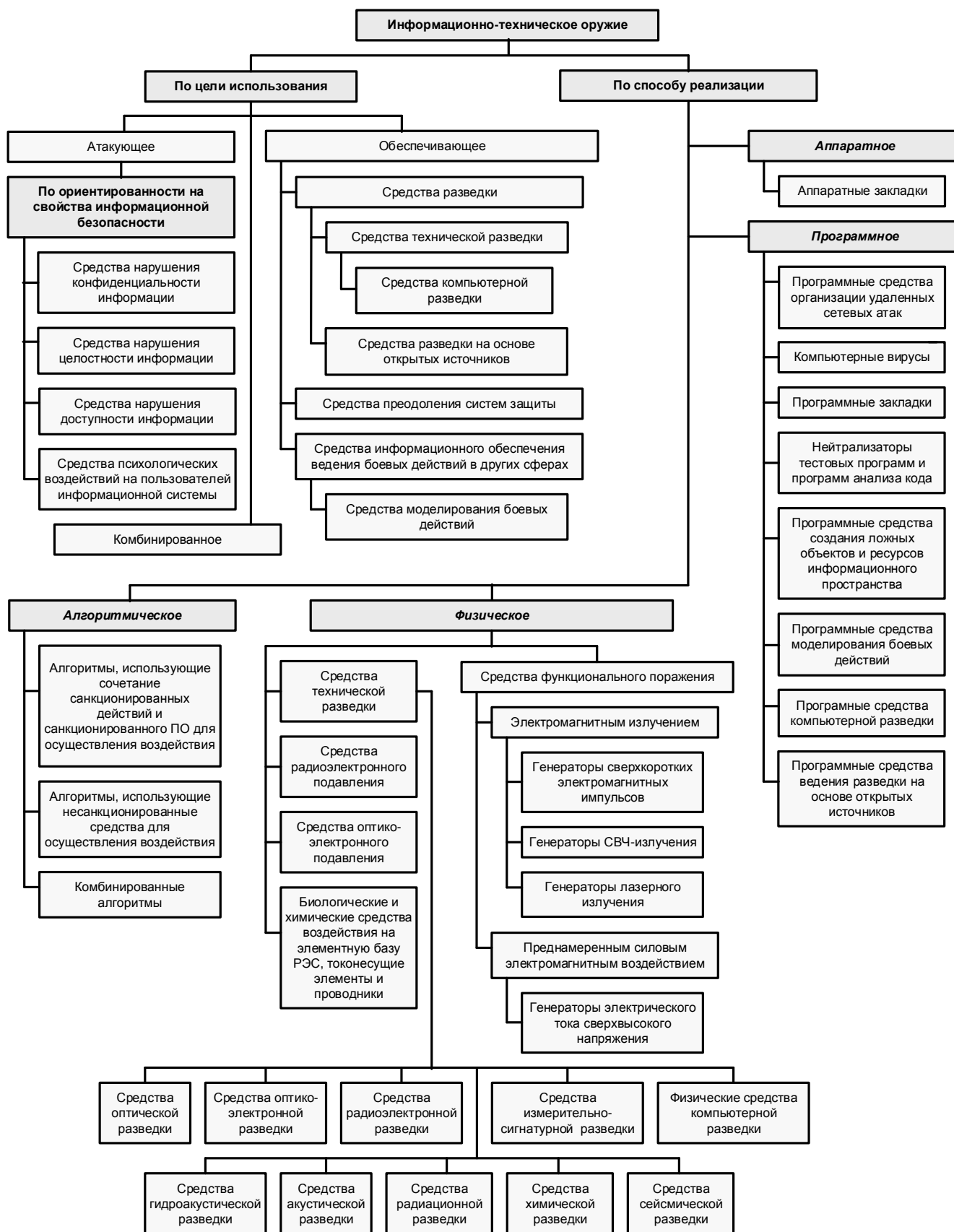


Рис. 1. Классификация информационно-технического оружия

Обеспечивающее информационно-техническое оружие применяется для сбора данных, обеспечивающих эффективное применение оборонительного или атакующего информационно-технического и другого оружия, а также против средств защиты атакуемой системы [2].

Обеспечивающее информационно-техническое оружие можно разделить на:

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;

2) средства преодоления систем защиты;

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

Необходимо отметить, что средства разведки почти всегда выступают в качестве обеспечивающего оружия. Они позволяют получить информацию об атакующих средствах информационно-технического 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, связанные 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.

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 комплексы для моделирования боевых действий, которые позволяют путем многократного прогона модели найти рациональный состав сил и средств, а также оптимальную стратегию их действий при любом вероятном сценарии действий противника.

Атакующее информационно-техническое оружие – оружие, с помощью которого осуществляется воздействие на хранимую, обрабатываемую и передаваемую в системе информацию, нарушающее используемые в системе информационные технологии [2].

Атакующее информационно-техническое оружие, в зависимости от его ориентированности на нарушение конкретного свойства информационной безопасности, можно разделить на четыре основных вида [2]:

- средства нарушения конфиденциальности информации;
- средства нарушения целостности информации;

- средства нарушения доступности информации;
- средства психологических воздействий на пользователей информационной системы.

Применение атакующего информационно-технического оружия направлено на срыв выполнения информационной системой целевых задач.

Как правило, атакующее информационно-техническое оружие включает в себя следующие компоненты, объединенные в единую систему [19]:

- средство доставки оружия;
- средство преодоления подсистемы защиты атакуемой системы;
- полезная нагрузка.

2. По способу реализации информационно-техническое оружие можно разделить на следующие классы [2, 7]:

- алгоритмическое;
- программное;
- аппаратное;
- физическое.

Информационно-техническое оружие, относящееся к разным классам, может применяться совместно. Кроме того, некоторые виды информационно-технического оружия могут одновременно нести в себе черты нескольких классов.

К **алгоритмическому информационно-техническому оружию** относятся [2]:

- алгоритмы, использующие сочетание санкционированных действий и санкционированного (легального) программного обеспечения для осуществления 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 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.

Примером алгоритмического оружия является DoS-атака (Denial of Service – отказ в обслуживании) заключающаяся в том, что на атакуемую систему с высокой интенсивностью посылаются корректные запросы на использование ее информационных ресурсов. Это ведет к тому, что возможности информационной системы по обслуживанию таких запросов

быстро исчерпываются, и она отказывает в обслуживании всем своим пользователям.

К **программному информационно-техническому оружию** относятся программное обеспечение, которое может быть использовано для проведения атак на информационные системы противника, и позволяющее в процессе своей работы производить несанкционированное воздействие на ее информационные ресурсы. К такому программному обеспечению можно отнести:

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

Кроме того, к программному информационно-техническому оружию можно отнести ряд программных средств, решающих обеспечивающие задачи, как в информационном пространстве, так и 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;
- программные средства ведения разведки по открытым источникам в семантической части информационного пространства.

К **аппаратному информационному оружию** могут быть отнесены 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.

К **физическому информационно-техническому оружию** могут быть отнесены средства добывания информации путем доступа к физической инфраструктуре информационного пространства, анализу генерируемых этой инфраструктурой физических полей, а также средства радиоэлектронного и огневого поражения ее физических элементов. При этом, некоторые специалисты считают более корректным отнесение к физическому информационно-техническому оружию только средств, предназначенных исключительно для воздействия на технические элементы информационной системы.

Обобщение сведений, представленных в работах [7, 13] показал, что классификация физического информационно-технического оружия может иметь вид:

- средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
- 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.;
- средства функционального поражения преднамеренными силовыми электромагнитными воздействиями – генераторы электрического тока сверхвысокого напряжения;
- биологические и химические средства воздействия на элементную базу радиоэлектронных систем (РЭС), их токонесущие элементы и проводники (например, графитовые бомбы).

2.2 Определение и классификация информационно-технических воздействий

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

Объекты информационно-технического 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.

Различают следующие **виды информационно-технических воздействий**:

- одиночные;
- групповые.

Информационно-технические воздействия также классифицируют по характеру поражающих свойств [2, 10]:

- 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 информационно-технические воздействия могут быть:

- пассивными:
 - перехват;
 - несанкционированный доступ;
- активными:
 - разрушающие воздействия;
 - манипулирующие воздействия;

- блокирующие воздействия;
- отвлекающие.

Пассивные воздействия не оказывают непосредственного влияния на работу информационной системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование информационной системы приводит к тому, что пассивное воздействие трудно обнаружить. Примером пассивного воздействия является разведка параметров информационной системы.

Активные воздействия оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Очевидной 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.

По цели использования информационно-технические воздействия могут быть классифицированы на:

- обеспечивающие;
- атакующие;
- оборонительные;
- комбинированные.

По способу реализации информационно-технические воздействия могут быть разделены на:

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

Классификация информационно-технических воздействий в общем случае по смыслу совпадает с классификацией информационно-технического оружия, за исключением оборонительных воздействий. Традиционно, средства оборонительных информационно-технических воздействий не рассматриваются в качестве оборонительного информационно-технического оружия, вместе с тем они существуют и играют одну из ведущих ролей в информационном противоборстве при организации защиты собственной стороны.

Оборонительные информационно-технические воздействия ориентированы на противодействие информационно-техническому оружию противника. Их можно классифицировать следующим образом:

- *выявляющие* – воздействия, ориентированные на выявление как самого факта, так и последовательности атакующих воздействий противника;
- *блокирующие* – воздействия, ориентированные на блокировку атакующих воздействий противника;
- *контр-атакующие* – воздействия на информацию, информационные ресурсы и информационную инфраструктуру противника с целью 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* – способы маскировки, обеспечения безопасности, повышения скрытности реальных режимов функционирования, а также мониторинга каналов утечки в отношении собственных информационных систем.

Схема классификации информационно-технических воздействий представлена на рис. 2.

Средства информационно-технического воздействия – средства, используемые в качестве информационно-технического оружия или для защиты от него [2].

Необходимо отметить, что классификация атакующих и обеспечивающих информационно-технических воздействий в общем виде совпадает с классификацией соответствующих видов информационно-технического оружия. Однако необходимость защиты от атакующих и обеспечивающих информационно-технических воздействий противника позволяет дополнительно выделить так называемые оборонительные средства информационно-технического воздействия, к которым можно отнести:

- средства антивирусной защиты;
- системы обнаружения и предотвращения вторжений;
- средства криптографической защиты;
- стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
- средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недеклалируемых возможностей;
- средства тестирования программного обеспечения и анализа кода для выявления программных закладок и недеклалируемых возможностей;
- средства создания ложных объектов и ресурсов в информационном пространстве.

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

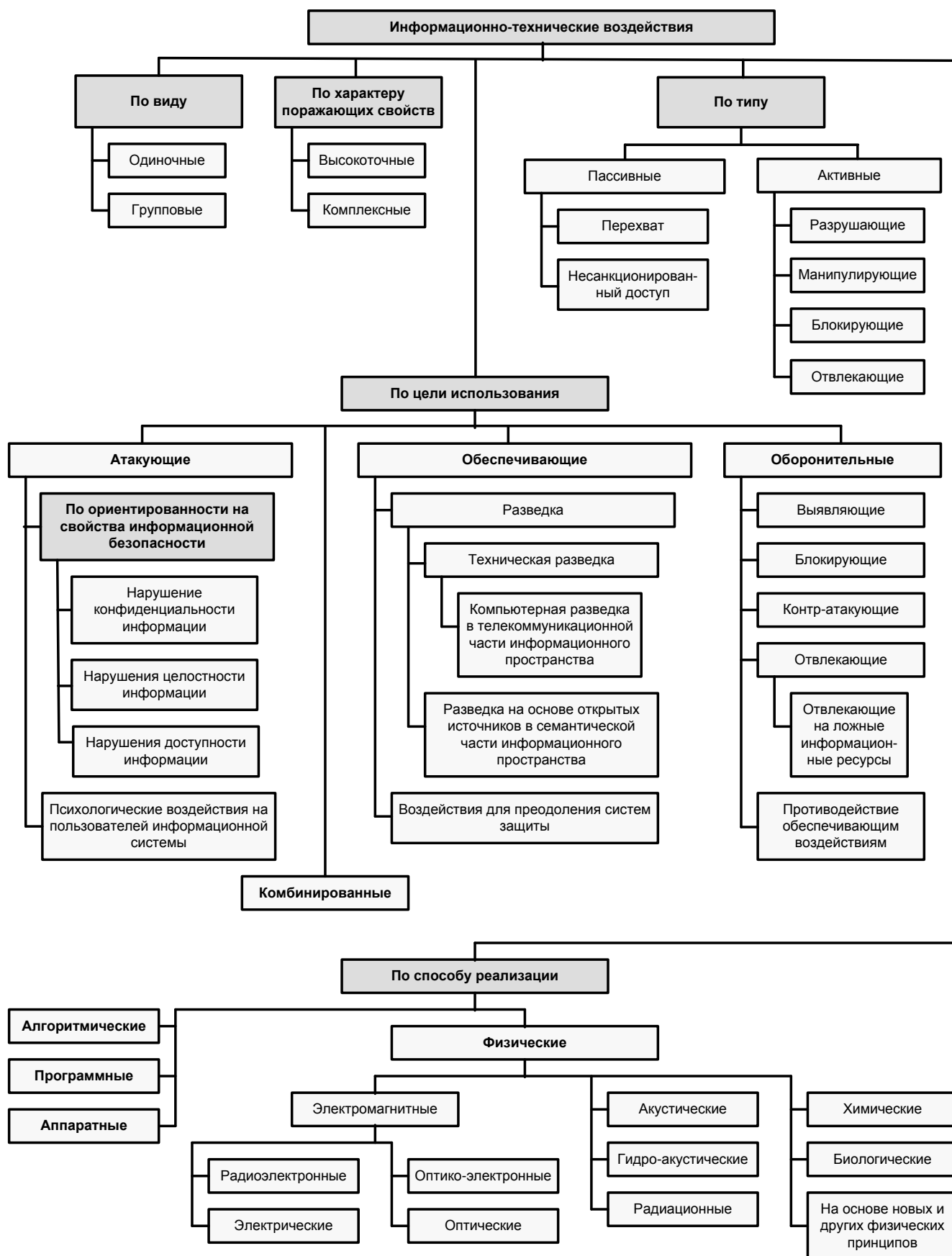


Рис. 2. Классификация информационно-технических воздействий

Средства специального программно-математического воздействия – некоторая программа или комплекс программ, способные выполнить любое подмножество перечисленных ниже функций [2, 20]:

- скрывать признаки своего присутствия в программно-аппаратной среде информационной системы;
- обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать) код программ в памяти информационной системы;
- 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;
- подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию, передаваемую по каналам управления;
- противодействовать работе тестовых программ и систем защиты информационных ресурсов.

При этом под самокопированием понимается процесс воспроизведения своего собственного кода (в том числе и в модифицированном виде) в оперативной или внешней памяти системы с последующим его внедрением. Под ассоциированием с другой программой понимается интеграция своего кода, либо его части в код другой программы таким образом, чтобы при некоторых условиях управление передавалось на код программы с потенциально опасными последствиями [2].

К основным средствам информационно-технического воздействия, классифицированным по способу реализации, можно отнести:

1) алгоритмические (атакующие):

- эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйверы, BIOS);
- эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
- эксплойты, ориентированные на сетевые протоколы информационной системы;
- 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 от

промышленного контролера, в течение длительного времени задавал для центрифуг нештатный режим работы, что привело к отказу более 1000 центрифуг на Иранском заводе по обогащению урана);

2) программные:

- 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;
 - программные средства ведения разведки на основе открытых источников в семантической части информационного пространства;
- оборонительные:
 - программные средства антивирусной защиты;
 - системы обнаружения и предотвращения вторжений;
 - программные средства криптографической защиты;
 - программные стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
 - 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:

- атакующие:
 - аппаратные закладки;
- оборонительные:
 - средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;

4) физические:

- атакующие:
 - средства РЭП;
 - 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 РЭС, токонесущие элементы и проводники (например, графитовые бомбы).
 - обеспечивающие:
 - средства технической разведки (в том числе и средства компьютерной разведки).

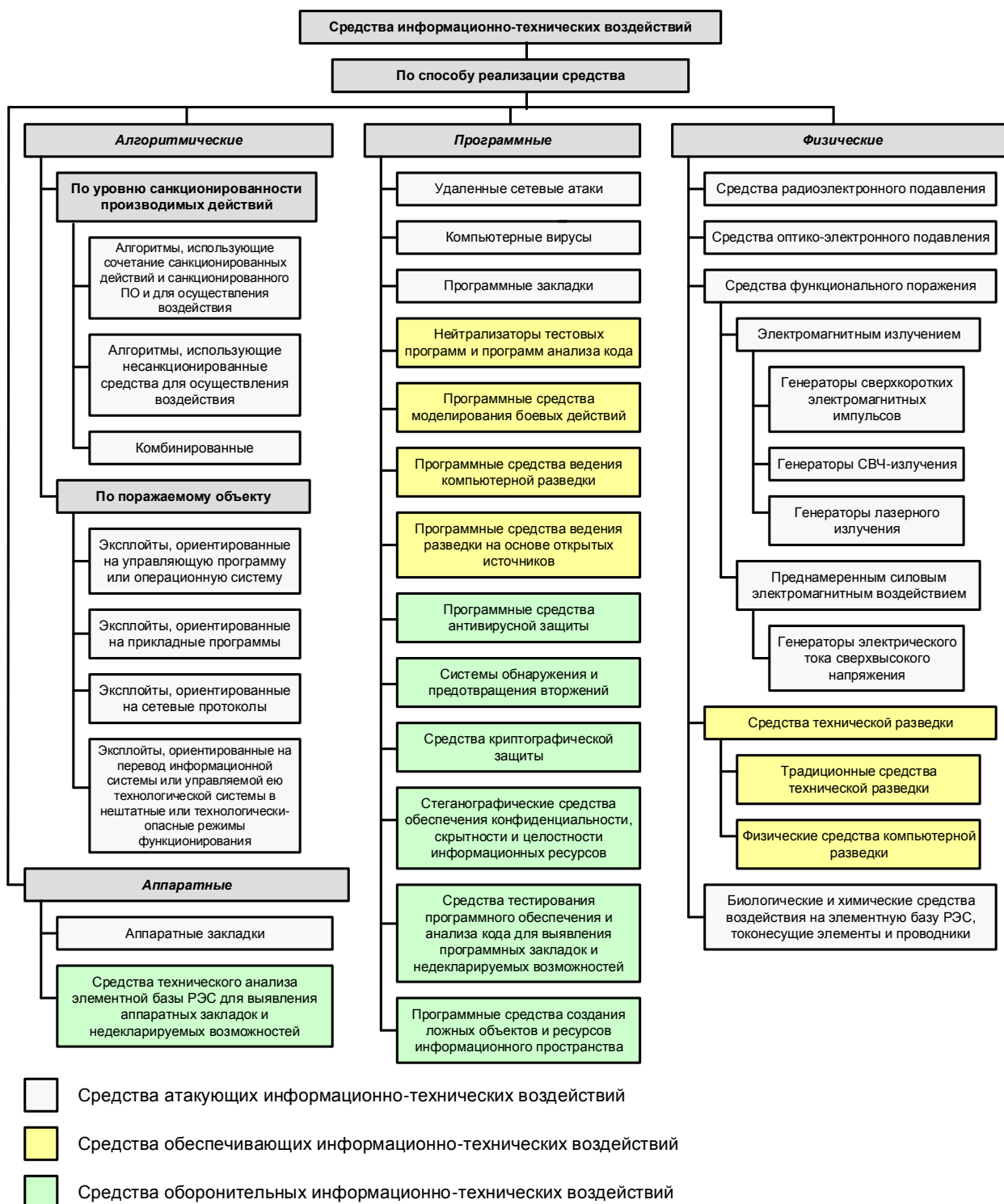


Рис 3. Классификация средств информационно-технического воздействия

Отдельно необходимо отметить следующее. К средствам технической разведки, представленным в данной классификации, относятся те средства, которые добывают информацию об атакующих средствах информационно-технического оружия противника и способах его применения, т.е. являются средствами обеспечивающего информационного оружия. Средства технической разведки могут оказывать воздействие на объекты противника как путем пассивных действий, направленные на добывание информации, что, как правило, связано с нарушением ее конфиденциальности, так и путем активных действий (атак), направленных на создание условий, благоприятствующих добыванию информации.

Схема классификации средств информационно-технических воздействий представлена на рис. 3.

Рассмотрим более подробно наиболее распространенные средства информационно-технического воздействия из представленных на рис. 3. Виду 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 [21]), то основное внимание уделим следующим информационно-техническим 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 моделирования боевых действий;
- средства технической разведки (средства компьютерной разведки рассмотрены отдельно);
- средства разведки по открытым источникам в глобальном информационном пространстве.

3. Наиболее распространенные средства информационно-технического воздействия

3.1 Удаленные сетевые атаки

3.1.1 Определение и классификация удаленных сетевых атак

С учетом определения и классификации удаленных воздействий на распределенные вычислительные системы, представленные в работе [22], можно дать следующее определение.

Удаленная сетевая атака – это разрушающее или дестабилизирующее информационно-техническое 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 уязвимостям в существующих протоколах обмена данными и в подсистемах защиты распределенных информационных систем. При этом к основным уязвимостям информационных систем, которые позволяют проводить против них успешные удаленные сетевые атаки, относятся [21, 22]:

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

В соответствии с различными основаниями удаленные сетевые атаки можно классифицировать следующим образом (рис. 4).

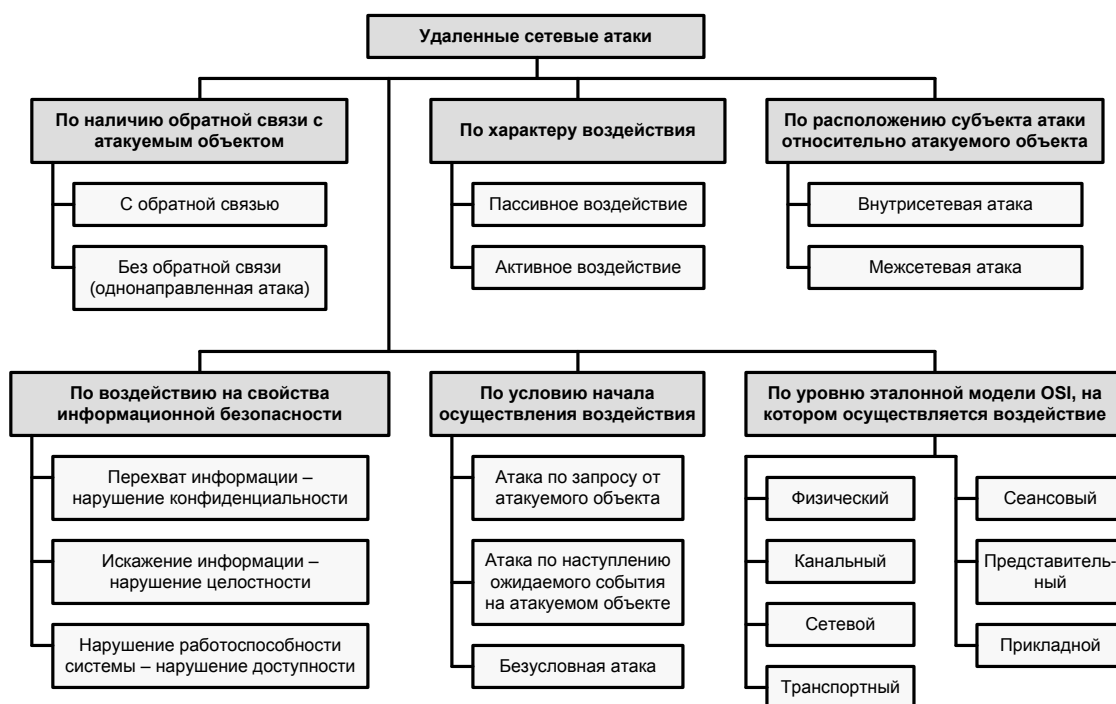


Рис. 4. Классификация удаленных сетевых атак

1. По характеру воздействия [21, 22]:

- пассивное воздействие;
- активное воздействие.

Пассивное воздействие не оказывает непосредственного 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. Примером типовой пассивной удаленной сетевой атаки является прослушивание канала связи.

Активное воздействие оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Практически все 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 [21, 22]:

- 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 невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. В этом случае 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 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. Таким образом, искажение информации ведет к нарушению целостности информационных ресурсов системы. Примером удаленной сетевой атаки, целью которой является нарушение целостности информационных ресурсов, может служить атака, связанная с внедрением ложного сетевого объекта в систему, например внедрения ложного DNS-сервера.

При нарушении работоспособности системы атакующей стороной не предполагается 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 [21, 22]:

- 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 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 [21, 22]:

- 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 запросов, 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 [21, 22]:

- 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 мерам по отражению атаки.

6. По уровню эталонной модели OSI, на котором осуществляется воздействие [21, 22]:

- физический;
- канальный;
- сетевой;
- транспортный;
- сеансовый;
- представительный;
- прикладной.

Удаленные атаки могут быть ориентированны 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 каналы 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. Либо DoS-атака на узловое оборудование сети, либо вирус поражающий операционную систему конечного терминального оборудования.

3.1.2 Примеры способов информационно-технических воздействий на основе удаленных сетевых атак

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

К основным способам и средствам информационно-технического воздействия, которые можно классифицировать как удаленные сетевые атаки, относятся (рис. 5) [21, 22]:

- 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»:
 - отказ в обслуживании (DoS-атака);
 - распределенная атака «отказ в обслуживании» (DDoS-атака);
 - заикливание процедуры обработки запроса.

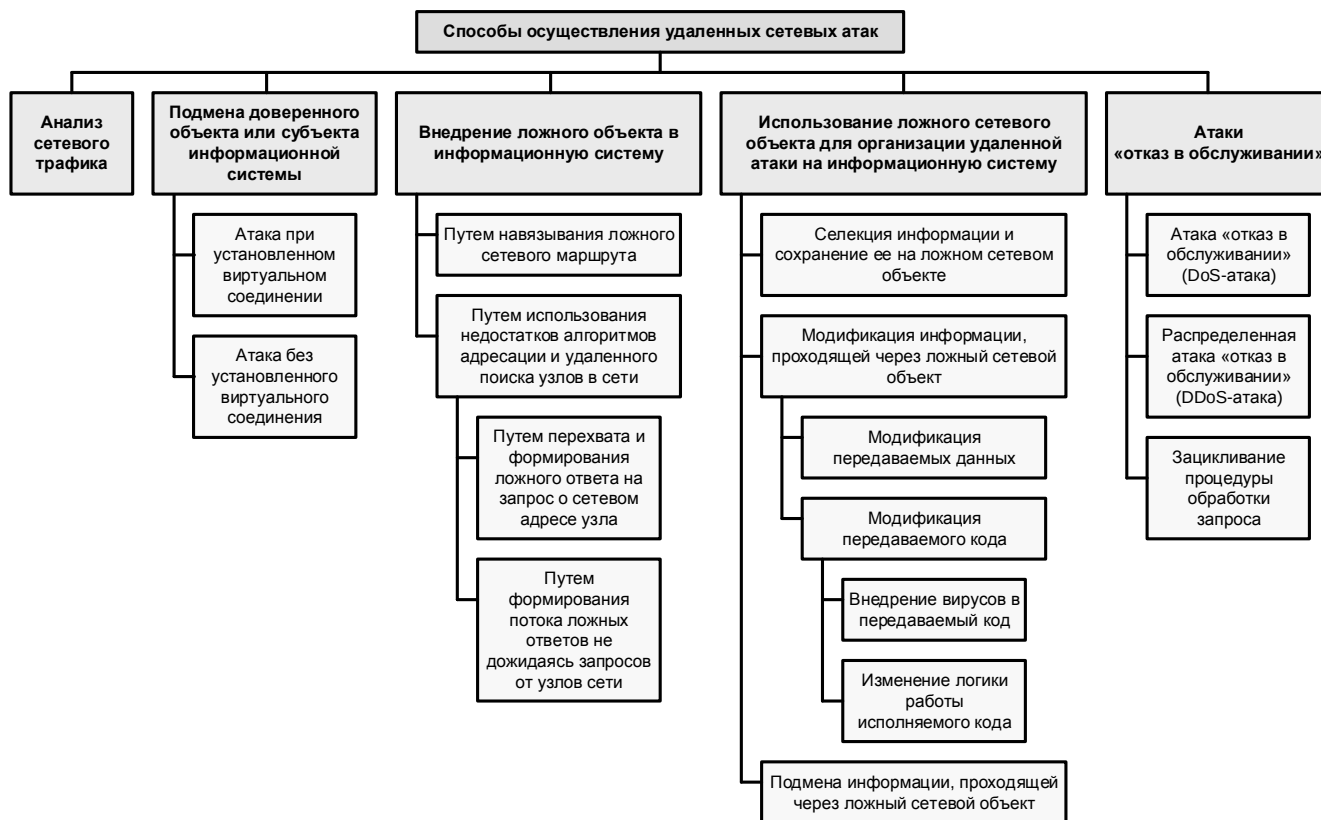


Рис. 5. Классификация способов осуществления удаленных сетевых атак

Анализ сетевого трафика. Основной особенностью сетевой информационной системы является то, что ее объекты распределены в пространстве и связь между ними осуществляется по сетевым соединениям. Таким образом, сообщения и данные, пересылаемые между объектами информационной системы, передаются по каналам связи в виде пакетов. Эта особенность привела к появлению специфичного для сетевой информационной

системы удаленного воздействия, заключающегося в прослушивании канала связи. Данное воздействие называется *анализом сетевого трафика*.

Анализ сетевого трафика позволяет [21, 22]:

- изучить логику работы сетевой информационной системы, то есть получить взаимно однозначное соответствие событий, происходящих в системе, команд и данных, пересылаемых друг другу ее объектами, в момент появления этих событий. Это достигается путем перехвата и анализа пакетов сетевого трафика. Знание логики работы информационной системы позволяет смоделировать и осуществлять другие удаленные сетевые атаки;
- перехватить поток данных, которыми обмениваются объекты сетевой информационной системы. Таким образом, эта атака заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером информации, перехваченной при помощи данной типовой удаленной атаки, могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети.

В соответствии с выше представленной классификацией анализ сетевого трафика является пассивным воздействием. Осуществление данной атаки без обратной связи ведет к нарушению конфиденциальности информации внутри одного сегмента сети на канальном или сетевом уровне OSI. При этом начало осуществления атаки безусловно по отношению к цели атаки [21, 22].

Подмена доверенного объекта или субъекта информационной системы. Одной из проблем безопасности сетевой информационной системы является недостаточная идентификация и аутентификация ее объектов удаленных друг от друга. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами сетевого взаимодействия. Обычно в сетевых информационных системах эта проблема решается следующим образом – в процессе создания виртуального канала объекты системы обмениваются определенной информацией, уникально идентифицирующей данный канал. Однако такой обмен производится не всегда. Зачастую, особенно при передаче служебной и адресной информации в сети, используются одиночные сообщения, не требующие подтверждения. Так как сетевой адрес достаточно просто подделывается, его можно использовать для виртуальной подмены доверенного объекта или субъекта информационной системы. Таким образом, в том случае, когда в сети используются нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной удаленная атака *подмена доверенного объекта или субъекта информационной системы*, заключающаяся в передаче по сети сообщений от имени произвольного объекта или субъекта информационной системы [21, 22].

Существуют две разновидности этой сетевой атаки, в зависимости от принятой в системе политики информационной безопасности и подхода к защите сетевых соединений [21, 22]:

- атака при установленном виртуальном соединении;
- атака без установленного виртуального соединения.

В случае если в сети для сеанса обмена данными устанавливаются виртуальные соединения, атака будет заключаться в присвоении прав доверенного субъекта сетевого взаимодействия, легально подключившегося к объекту системы. Это позволит атакующему вести сеанс работы с объектом информационной системы от имени доверенного субъекта. Реализация таких удаленных атак обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты системой как корректные). Однако, для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сетевых сообщений [21, 22].

Атаки на информационную систему, в которой не используются виртуальные соединения, заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов. В этом случае возможна подделка сетевого адреса отправителя. Например, так реализуется удаленная атака, использующая навязывание ложного маршрута, путем посылки ложных адресных сообщений [21, 22].

Подмена доверенного объекта или субъекта информационной системы может быть классифицирована как активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации по наступлению на атакуемом объекте определенного события. Такая удаленная атака может являться как внутрисетевой, так и межсетевой, как с обратной связью, так и без обратной связи с атакуемым объектом и осуществляться на сетевом или транспортном уровнях модели OSI [21, 22].

Внедрение ложного объекта в информационную систему. Зачастую в распределенной информационной системе бывают недостаточно надежно решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов), при их взаимодействии с объектами системы. В этом случае такая распределенная система может подвергнуться сетевой атаке, связанной с изменением параметров маршрутизации и внедрением в сеть ложного объекта. В том случае, если настройки сети таковы, что для взаимодействия объектов необходимо использовать алгоритмы удаленного поиска узлов, то это также может быть использовано для внедрения в систему ложного объекта.

Таким образом, существуют два принципиально разных способа проведения атаки «внедрение ложного объекта в информационную систему» [21, 22]:

- 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.

Современные глобальные сети представляют собой совокупность сетевых сегментов, связанных между собой через узлы-маршрутизаторы. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждой пары адресатов сети указывается оптимальный маршрут. Основная цель атаки, связанной с внедрением ложного объекта путем навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте сетевой информационной системы так, чтобы новый маршрут проходил через ложный объект сети – узел атакующего. Реализация этой атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. Данная атака проходит в две стадии [21, 22].

1. Атакующему необходимо от имени сетевых управляющих устройств (например, маршрутизаторов) произвести рассылку по сети специальных служебных сообщений, что приведет к изменению маршрутизации в сети. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, который будет проходить через его узел.
2. Атакующий наращивает количество трафика, перенаправленного через свой узел, и получает возможность вести прием, анализ и передачу сообщений, передаваемых по сети.

Внедрение ложного объекта путем навязывания ложного сетевого маршрута – активное воздействие, безусловное по отношению к цели атаки. Данная удаленная атака может осуществляться как внутри одного сегмента сети, так и межсетевым образом, как с обратной связью, так и без обратной связи с атакуемым объектом на сетевом, транспортном и прикладном уровне модели OSI [21, 22].

В распределенной информационной системе часто оказывается, что ее удаленные объекты изначально не имеют достаточно информации, необходимой для адресации передаваемых сообщений. Обычно такой информацией являются аппаратные и логические адреса объектов системы. Для получения подобной информации в распределенных системах используются различные алгоритмы удаленного поиска, заключающиеся в передаче по сети специальных поисковых запросов. После получения ответа на запрос, запросивший субъект системы обладает всеми необходимыми данными для адресации. Руководствуясь полученными из ответа сведениями об искомом объекте, запросивший субъект системы начинает передачу информации. Примером подобных запросов, на которых базируются алгоритмы удаленного поиска, могут служить ARP- и DNS-запросы в сети Internet [21, 22].

В случае использования в распределенной информационной системе механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать

данные, использование которых приведет к адресации на атакующий ложный узел. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через этот ложный объект информационной системы [21, 22].

Другой вариант внедрения в распределенную информационную систему ложного объекта использует недостатки алгоритма удаленного сетевого поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса, и тогда его ложный ответ будет немедленно принят и обработан. Такая удаленная атака чрезвычайно распространена в глобальных сетях, когда у атакующего, из-за нахождения его в другом сетевом сегменте относительно цели атаки, просто нет возможности перехватить поисковый запрос [21, 22].

Внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети – активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации, которое может являться атакой по запросу от атакуемого объекта, а также безусловной атакой. Данная удаленная атака может быть как внутрисетевой, так и межсетевой, имеет обратную связь с атакуемым объектом и осуществляется на канальном, сетевом и прикладном уровнях модели OSI [21, 22].

Использование ложного объекта для организации удаленной атаки на систему. После внедрения ложного объекта в сеть и получением контроля над проходящим потоком информации в сети, ложный объект может применяться для различных способов воздействия на перехваченную информацию. Выделяют следующие основные воздействия на информацию, перехваченную ложным объектом [21, 22]:

- селекция информации и сохранение ее на ложном сетевом объекте;
- модификация информации, проходящей через ложный сетевой объект;
- подмена информации, проходящей через ложный сетевой объект.

Селекция информации и сохранение ее на ложном сетевом объекте является пассивной сетевой атакой, сходной с атакой «анализ сетевого трафика», которая дополнена динамическим семантическим анализом, производимом на ложном объекте. Вместе с тем наибольший интерес представляет возможность использования ложного объекта для модификации или подмены информации.

Рассматривают два основных вида модификации информации [21, 22]:

- модификация передаваемых данных;
- модификация передаваемого кода:
 - внедрение вирусов в передаваемый код;
 - изменение логики работы исполняемого кода.

Для модификации передаваемых данных на внедренном объекте производится селекция потока перехваченной информации и его анализ. При этом может быть распознан тип передаваемых файлов (исполняемый файл или файл, содержащий данные). При обнаружении файла данных появляется

возможность модифицировать эти данные, проходящие через ложный объект. При этом если модификация данных является достаточно стандартным воздействием, то на модификации передаваемого кода стоит остановиться отдельно.

Ложный объект, проводя семантический анализ информации, проходящей через него, может выделять среди потока информации файлы, содержащие исполняемый код. Для того, чтобы определить, что передается по сети – код или данные, необходимо распознавать определенные особенности, свойственные конкретным типам исполняемых файлов. При этом можно выделить два различных по цели вида модификации кода [21, 22]:

- внедрение вирусов в передаваемый код;
- изменение логики работы исполняемого кода.

При внедрении вирусов в передаваемый код к исполняемому файлу дописывается тело вируса, а также изменяется точка начала исполнения кода так, чтобы она указывала на начало кода внедренного вируса. Описанный способ, в принципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что файл оказывается заражен вирусом в момент передачи его по сети! Такое возможно лишь при использовании воздействия «внедрение ложного объекта» [21, 22].

При изменении логики работы исполняемого файла, при передаче его по сети происходит похожая модификация исполняемого кода. Однако ее цель – алгоритмическое воздействие, ориентированное на внедрение программных закладок, внесение в исполняемый файл дополнительных уязвимостей или эксплойтов. Сложностью такого воздействия является то, что для него, как правило, требуется предварительное исследование логики функционирования исполняемого файла [21, 22].

Внедрение ложного объекта позволяет не только модифицировать, но и подменять перехваченную им информацию. При возникновении в сети определенного контролируемого ложным объектом события, одному из участников обмена посылается заранее подготовленная дезинформация. При этом такая дезинформация, в зависимости от контролируемого события, может быть как исполняемым кодом, так и данными.

Отказ в обслуживании. В общем случае в сетевой информационной системе каждый ее субъект должен иметь возможность подключиться к любому объекту системы и получить в соответствии со своими правами удаленный доступ к его информационным ресурсам. Обычно в сетевых информационных системах возможность предоставления удаленного доступа реализуется следующим образом – на объекте системы запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. В случае получения запроса на соединение сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. Очевидно, что сервер способен отвечать лишь на ограниченное число запросов. Эти ограничения зависят от параметров информационной системы, пропускной способности ее сети и быстродействия ЭВМ, на которых он функционирует.

Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов за счет отправки большого числа запросов к нему.

Различают три типа этих удаленных атак.

1. *Отказ в обслуживании (DoS-атака)* – передача с одного адреса такого количества запросов на атакуемый объект, которое позволяет передать пропускная способность канала связи. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) системы, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная блокировка объекта из-за невозможности системы заниматься ничем другим, кроме обработки запросов.
2. *Распределенная атака «отказ в обслуживании» (DDoS-атака)* – передача с нескольких объектов системы на другой атакуемый объект бесконечного числа запросов на подключение от имени этих или других объектов. Результатом применения этой удаленной атаки является нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов сетевой информационной системы.
3. *Защивание процедуры обработки запроса* – передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно переполнение буфера с последующим зависанием системы.

Удаленная сетевая атака «отказ в обслуживании» классифицируется как активное воздействие, осуществляемое с целью нарушения работоспособности системы, безусловная относительно цели атаки. Данная атака является однонаправленным воздействием, осуществляемым как межсетевым, так и внутрисетевым образом, осуществляемым на сетевом, транспортном и прикладном уровнях модели OSI [21, 22].

Наиболее распространенными способами осуществления атаки «отказ в обслуживании» являются следующие (рис. 6).

1. Способы, основанные на насыщении полосы пропускания системы – атаки, связанные с большим количеством, как правило, бессмысленных или сформированных в неправильном формате запросов к информационной системе или ее сетевому оборудованию, с целью обеспечить отказ в работе системы из-за исчерпания ее системных ресурсов (процессорного времени, памяти или пропускной способности каналов связи). К наиболее распространенным таким способам относятся [23]:

- атаки типа HTTP-flood и ping-flood;
- Smurf-атака (ICMP-flood);
- атака с помощью переполнения пакетами SYN в TCP соединении (SYN-flood).



Рис. 6. Наиболее распространенные способы осуществления атаки «отказ в обслуживании»

2. Способы, основанные на недостатке ресурсов системы – атаки, связанные с захватом или избыточным использованием ресурсов информационной системы. К наиболее распространенным таким способам относятся [23]:

- отправка «тяжелых» или «сложных» пакетов;
- переполнение сервера log-файлами;
- использование уязвимостей неправильно настроенной подсистемы управления кодами использования системных ресурсов;
- использование уязвимостей недостаточной проверки данных пользователей;
- атаки, вызывающие ложные срабатывания подсистемы защиты информационной системы.

3. Способы, основанные на удаленном несанкционированном доступе за счет использования эксплойтов в программном обеспечении атакуемой системы. К наиболее распространенным таким способам относятся [23]:

- удаленное использование уязвимостей в программном коде операционной системы и прикладного программного обеспечения информационной системы;
- удаленное использование переполнения буфера программы;
- удаленное использование ошибок в разделении памяти между программами в защищенном режиме операционной системы.

4. Способы, основанные на использовании эксплойтов сетевых протоколов атакуемой системы. К наиболее распространенным таким способам относятся [23]:

- DoS-атаки, использующие уязвимости в программном обеспечении DNS-серверов;
- DDoS-атаки на DNS-серверы.

В настоящее время атаки типа «отказ в обслуживании» являются не только наиболее распространенными, но и наиболее опасными воздействиями. Так, в ноябре 2002 года была проведена глобальная DDoS-атака на корневые DNS-серверы с целью полного блокирования общедоступного сегмента сети Интернет. В результате этой атаки злоумышленники смогли вывести из строя 7 из 13 корневых DNS-серверов [23].

3.2 Компьютерные вирусы

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве боевых средств информационно-технического воздействия начато сравнительно недавно. При этом, несмотря на относительную молодость информационно-технических воздействий вирусного типа, уже зафиксировано несколько «волн» их применения для достижения стратегических целей. К первому случаю такого использования вируса относится применение в 2010 году вируса Stuxnet с целью срыва ядерной программы Ирана за счет инфицирования АСУ технологическим процессом обогащения урана. Как показывает анализ работ [24, 25, 26], к другим вирусам, которые также могут быть классифицированы как информационно-техническое оружие, можно также отнести: Flame, Duqu, Regin, Gauss, MiniFlame, MiniDuqu, Sputnik и др. Эксперты отмечают общие высокотехнологические черты данных вирусов, такие как: библиотеки (в том числе open source), среды, используемые уязвимости, приемы противодействия средствам защиты, а также высокое качество кода.

В отличие от своих «непрофессиональных собратьев» средства информационно-технического воздействия на основе вирусов обладают следующими особенностями функционирования [24]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей «нулевого» уровня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;
- гибкая система саморазмножения;
- инфраструктурная поддержка, обновление и управление;
- масштабируемость, наличие СУБД атак;
- высокое качество кода, и возможности обработки некорректных ситуаций.

Компьютерные вирусы в соответствии со способами распространения и вредоносной нагрузкой можно классифицировать по четырем основным типам [21]:

- классические вирусы;
- программы типа «червь»;
- программы типа «троян»;
- другие вредоносные программы.

Особенностью современных боевых вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам, и которые ориентированы на решение конкретной задачи (модули типа классический вирус – для саморазмножения в информационной системе, модули типа червь – для распространения по сети, модуль типа «троян» – для организации дестабилизирующего воздействия).

Кроме того, по способу хранения в памяти информационной системы компьютерные вирусы можно классифицировать на [27]:

- резидентные;
- нерезидентные.

Резидентные вирусы после активации хранят свои копии в оперативной памяти системы, способны перехватывать события операционной системы и программ (например, обращения к файлам или дискам) и инициировать при этом процедуры заражения обнаруженных объектов. Поэтому резидентные вирусы опасны не только во время работы инфицированной программы, но и после ее окончания. Резидентные копии таких вирусов остаются жизнеспособными вплоть до выключения или перезагрузки информационной системы [27].

Нерезидентные вирусы, напротив, активны на довольно непродолжительных интервалах времени – пока функционирует инфицированная вирусом программа [27].

Для защиты от обнаружения со стороны антивирусов и средств защиты информационной системы в вирусах могут применяться следующие технологии [21]:

- шифрование – вирус состоит из двух функциональных элементов: собственно, вирус и шифратор. При этом каждая конкретная копия вируса состоит из шифратора, собственного случайного ключа и собственно вируса, зашифрованного этим ключом;
- метаморфизм – создание различных копий вируса путем замены блоков команд на эквивалентные, путем перестановки местами участков кода, вставки между значащими участками кода незначащих команд и др.;
- перехват управления при обращении операционной системы или системы защиты к инфицированным элементам информационной системы.

Использование этих технологий маскировки вирусов привело к появлению следующих вирусов, которые классифицируются по технологии защиты от обнаружения [21]:

- шифрованный вирус – вирус, использующий простое шифрование своего тела со случайным ключом и неизменный шифратор. Такие вирусы могут быть обнаружены по сигнатуре шифратора;
- метаморфный вирус – вирус, применяющий метаморфизм ко всему своему телу для создания новых копий;
- полиморфный вирус – вирус, использующий метаморфный шифратор для шифрования тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм шифрования;
- стелс-вирус (stealth virus – вирус-невидимка) – вирус, полностью или частично скрывающий свое присутствие в системе путем перехвата обращений к операционной системе на осуществление чтения или записи в инфицированных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.) и подмены их содержимого с целью демонстрации подсистеме защиты оригинального содержимого объекта до его заражения.

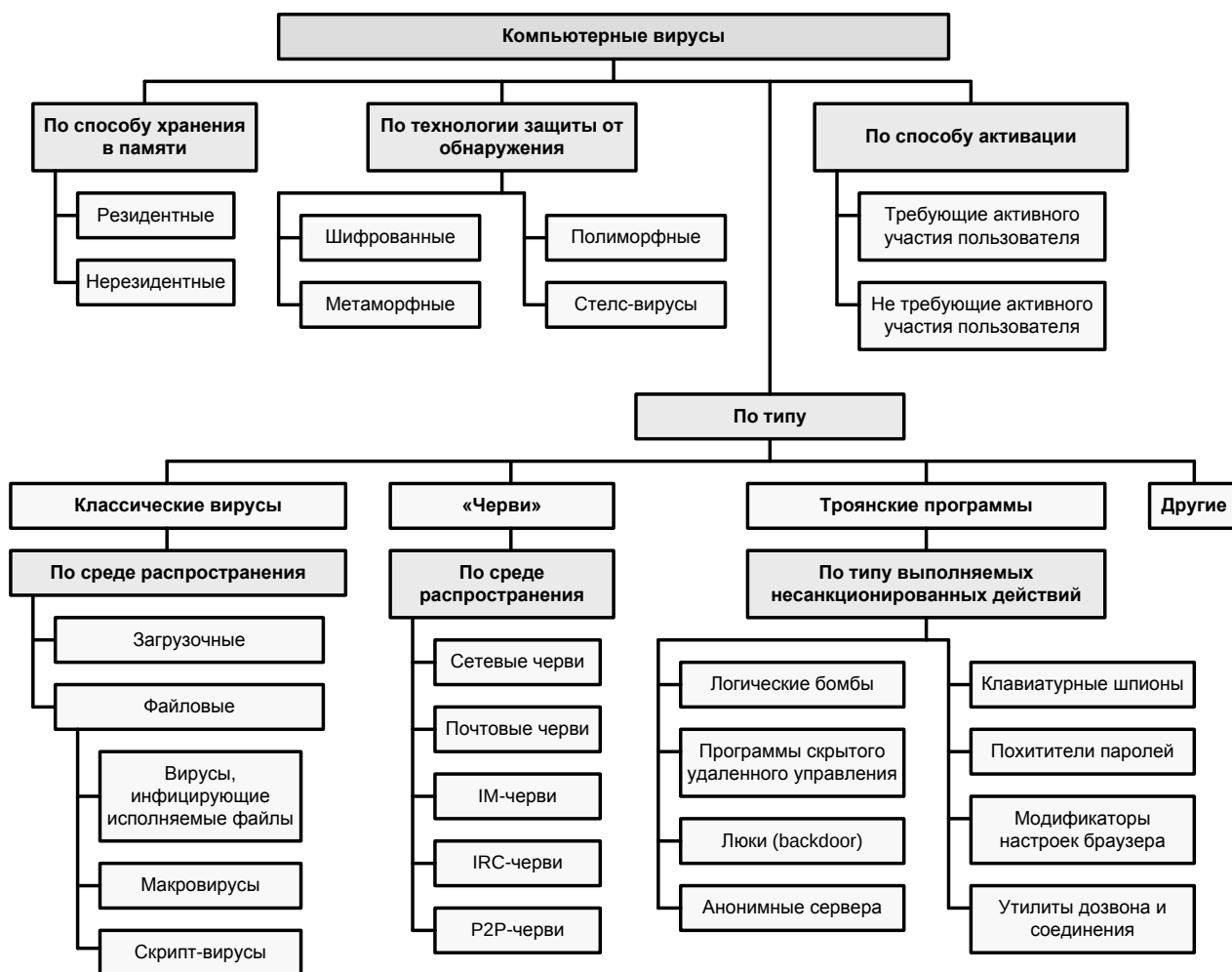


Рис. 7. Классификация компьютерных вирусов

Кроме того, компьютерные вирусы можно классифицировать по способу активации [21].

- Требующие активного участия пользователя. Отличительная особенность таких компьютерных вирусов является использование обманных методов. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добровольно открывает вложение с «почтовым червем», тем самым его активируя.
- Не требующие активного участия пользователя. Активация компьютерных вирусов без участия пользователя возможна за счет того, что вирус самостоятельно находит и использует уязвимости в безопасности информационной системы.

Общая схема классификации компьютерных вирусов представлена на рис. 7.

Рассмотрим основные особенности основных типов вирусов более подробно.

3.2.1 Классические вирусы

Основное свойство классического компьютерного вируса – это способность к саморазмножению [21].

Вирус – это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области операционных систем и прочие информационные ресурсы. При этом дубликаты сохраняют способность к дальнейшему распространению [21].

Условно жизненный цикл вируса можно разделить на пять стадий [21]:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- внедрение копий;

Пути проникновения вируса могут служить мобильные носители, сетевые соединения, а также любые другие каналы, по которым можно скопировать файл. Однако в отличие от «червей», вирусы не используют сетевые ресурсы – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал [21].

После проникновения следует активация вируса. В соответствии с выбранным методом активации вирусы делятся на следующие виды [21]:

- загрузочные вирусы – заражают загрузочные сектора жестких дисков и мобильных носителей;
- файловые вирусы – заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют следующие типы вирусов:
 - вирусы, инфицирующие исполняемые файлы – различными способами внедряются в исполняемые файлы программ

(внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы;

- макровирусы – инструкции, написанные на внутреннем языке команд заражаемого приложения (на, так называемых, макросах);
- скрипт-вирусы – инструкции, написанные на внутреннем языке для определенной командной оболочки (скриптов).

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан [21].

Основная цель вируса – распространение на другие ресурсы информационной системы и выполнение деструктивных действий при определенных событиях или действиях пользователя [21].

3.2.2 Черви

В отличие от классических вирусов программы типа «червь» – это вполне самостоятельные программы, которые также способны к саморазмножению, однако при этом они способны и к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин «сетевой червь» [21].

Программа типа «червь» – это программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению подсистем защиты информационных систем, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом [21].

Жизненный цикл «червей» состоит из следующих стадий [21]:

- проникновение в информационную систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

В зависимости от способа проникновения в систему «черви» классифицируются на следующие типы [21]:

- «сетевые черви» – используют для распространения локальные сети, каналы в информационно-вычислительных сетях, глобальные сети, в том числе и Интернет;
- «почтовые черви» – распространяются с помощью почтовых программ;
- «IM-черви» – используют для распространения системы мгновенного обмена сообщениями типа Internet Massager;
- «IRC-черви» – распространяются по каналам IRC (Internet Relay Chat) для обмена информацией в чатах и форумах;
- «P2P-черви» – распространяются при помощи пиринговых P2P файлообменных сетей.

Сетевые черви могут кооперироваться с вирусами – такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса) [21].

3.2.3 Троянские программы

В отличие от вирусов и червей в программах типа «троянский конь» не всегда предусмотрен функционал саморазмножения. Довольно большая часть таких программ функцией саморазмножения вообще не обладает [21].

Программа типа «троян» («троянский конь») – программа, основной целью которой является вредоносное воздействие по отношению к информационной системе путем выполнения несанкционированных действий, а именно кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или несанкционированное использования его ресурсов [21].

Некоторые «трояны» способны к самостоятельному преодолению подсистемы защиты информационной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают в систему вместе с вирусом, либо с червем. В этом случае вирус или червь следует рассматривать как средство доставки, а «троян» – как средство информационного поражения [21].

Жизненный цикл «троянов» состоит всего из трех стадий [21]:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Как уже говорилось выше, проникать в информационную систему «трояны» могут двумя путями – самостоятельно и за счет кооперации с вирусом или сетевым червем. В первом случае может быть использована маскировка, когда «троян» выдает себя за полезное приложение, которое пользователь самостоятельно копирует и запускает. При этом программа-носитель действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные «трояну» [21].

Для проникновения в информационную систему «трояну» необходима активация, и здесь он похож на «червя» – либо требует активных действий от пользователя, либо самостоятельно заражает ее, используя уязвимости в защите информационной системы [21].

Программы типа «троян», как правило, классифицируются по типу выполняемых несанкционированных действий [21].

- Логические бомбы – характеризуются способностью при выполнении заранее заложенных в них условий (конкретный день, время суток, определенное действие пользователя или команда извне) выполнять несанкционированные действия по уничтожению или искажению информации, воспрепятствия доступа к тем или иным важным фрагментам информационного ресурса, либо дезорганизации работы технических средств.
- Программы скрытого удаленного управления – это «трояны», которые обеспечивают несанкционированный удаленный контроль над

инфицированной информационной системой. Такие программы предоставляют удаленному пользователю возможность скрытого исполнения программ в информационной системе, поиска, модификации и удаления информации, возможности скрыто загружать или отсылать информацию.

- Люки (backdoor) – программы, находящие или создающие уязвимости в защите информационной системы с целью дальнейшего предоставления удаленного несанкционированного доступа к ней. От программ удаленного управления этот тип «трояна» отличается более простой функциональностью и ориентированностью не на контроль системы, а на организацию доступа к ней. Как правило, данные «трояны» имеют функционал загрузки и запуска удаленных файлов. Это позволяет, при необходимости, загрузить на инфицированную систему программу скрытого удаленного управления и получить над информационной системой несанкционированный удаленный контроль.
- Анонимные сервера – разновидность «троянов», которые используют ресурсы зараженной информационной системы в своих целях, связанных с несанкционированной сетевой активностью: создание bot-сетей и управление ими, выполнение несанкционированных распределенных вычислений, организации и координация DDOS-атак, массовая отправка электронной почты, и другие подобные действия.
- Клавиатурные шпионы – находясь в оперативной памяти, записывают все данные, набираемые на клавиатуре с целью последующей их передачи.
- Похитители паролей – предназначены для кражи паролей и другой конфиденциальной информации путем поиска на зараженной системе специальных файлов, которые ее содержат.
- Модификаторы настроек браузера (программы просмотра информации в сети) – изменяют настройки браузера таким образом, чтобы стало возможным удаленное исполнение кода в браузере, доступ к хранящейся в нем конфиденциальной информации, подмена сертификатов безопасности, перенаправление на ложные страницы и т.п.
- Утилиты дозвона и соединения – в скрытом от пользователя режиме иницируют несанкционированное подключение к удаленным сервисам в сети.

Отдельно отметим, что существуют программы из класса «троянов», которые наносят вред другим, удаленным информационным системам и сетям, при этом, не нарушая работоспособности инфицированной системы. Примером таких программ могут служить анонимные сервера – организаторы DDoS-атак [21].

3.3 Программные закладки

Программная закладка – скрытно внедренная в защищенную информационную систему программа, либо намеренно измененный фрагмент программы, которая позволяет осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

При этом в большинстве случаев закладка внедряется самим разработчиком программного обеспечения для реализации в информационной системе некоторых сервисных или недекларируемых функций. Следовательно, под закладкой, как правило, понимается внутренний объект защищенной системы. Однако, в редких случаях, закладка может быть и внешним объектом по отношению к защищенной системе.

Программные закладки, получая несанкционированный доступ к данным в памяти информационной системы, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но в отличие от вирусов деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные. Довольно часто программные закладки выполняют роль перехватчиков паролей, сетевого трафика, а также служат в качестве скрытых интерфейсов для входа в систему. Однако, в отличие от вирусов, программные закладки не обладают способностью к саморазмножению, они встраиваются в ассоциированное с ними программное обеспечение и латентно функционируют вместе с ним. При этом, особенностью закладок, внедренных на стадии разработки программного обеспечения является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы [27].

Как и вирус, программная закладка должна скрывать свое присутствие в программной среде информационной системы. Однако программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами, выявляющими аномальное поведение и недекларируемые возможности программного обеспечения. В связи с этим, средства маскировки программных закладок преимущественно ориентированны на противодействие отладчикам программ, анализаторам кода и дисассемблерам. В качестве одного из широко применяемых способов маскировки является обфускация (запутывание) программ, в которые внедрена закладка [27].

Классификацию программных закладок можно провести по нескольким основаниям (рис. 8).

1. По месту внедрения в информационной системе программные закладки делятся на [27]:

- аппаратно-программные закладки, программно ассоциированные с аппаратными средствами (например, закладки в BIOS);
- загрузочные закладки, которые ассоциированы с программами начальной загрузки операционной среды информационной системы;

- драйверные закладки, которые ассоциированы с драйверами устройств информационной системы;
- прикладные закладки, которые ассоциированы с прикладным программным обеспечением общего назначения;
- исполняемые модули закладки, которые содержат только код программной закладки, который в дальнейшем внедряется в пакетные исполняемые файлы;
- закладки-имитаторы, имитирующие интерфейс служебных программ, работа с которыми предполагает ввод конфиденциальной информации;
- закладки, маскирующиеся под программы, позволяющие оптимизировать работу персонального компьютера, компьютерные игры и прочие развлекательные программы.

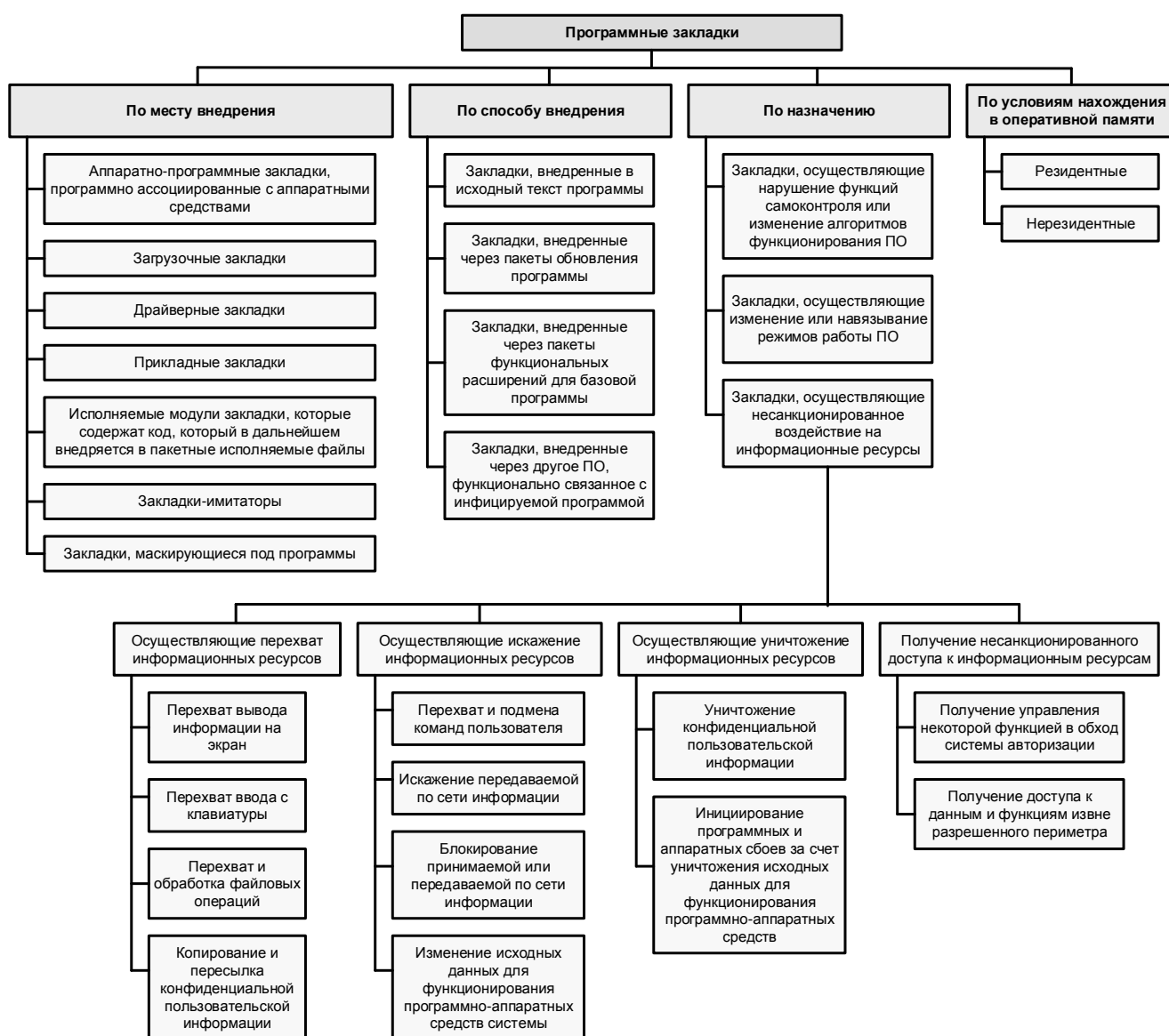


Рис. 8. Классификация программных закладок

2. По способу внедрения в программное обеспечение закладки можно классифицировать на:

- закладки, внедренные в исходный текст программы;
- закладки, внедренные через пакеты обновления программы;
- закладки, внедренные через пакеты функциональных расширений для базовой программы;
- закладки, внедренные через другое программное обеспечение, функционально связанное с инфицируемой программой;

3. По назначению программные закладки делятся на [27, 28]:

- закладки, осуществляющие несанкционированное воздействие на информационные ресурсы, которые находятся в оперативной или во внешней памяти системы, либо в памяти другой системы, подключенной по локальной или глобальной сети:
 - закладки, осуществляющие перехват информационных ресурсов:
 - перехват вывода информации на экран;
 - перехват ввода с клавиатуры;
 - перехват и обработка файловых операций;
 - копирование и пересылка конфиденциальной пользовательской информации;
 - закладки, осуществляющие искажение информационных ресурсов:
 - перехват и подмена команд пользователя;
 - искажение передаваемой по сети информации;
 - блокирование принимаемой или передаваемой по сети информации;
 - изменение исходных данных для функционирования программно-аппаратных средств системы;
 - закладки, осуществляющие уничтожение информационных ресурсов:
 - уничтожение конфиденциальной пользовательской информации;
 - инициирование программных и аппаратных сбоев за счет уничтожения исходных данных для функционирования программно-аппаратных средств;
 - получение несанкционированного доступа к информационным ресурсам:
 - получение управления некоторой функцией в обход системы авторизации;
 - получение доступа к данным и функциям извне разрешенного периметра;
- закладки, осуществляющие нарушение функций самоконтроля или изменение алгоритмов функционирования системных, прикладных и служебных программ;

- закладки, осуществляющие изменение или навязывание режимов работы программного обеспечения.

Для того, чтобы программная закладка начала функционировать, необходимо одновременное соблюдение двух условий, заставляющих систему исполнять команды, входящие в код программной закладки [27]:

- программная закладка должна попасть в оперативную память системы;
- должен быть выполнен ряд активизирующих условий, зависящих от типа программной закладки.

4. По условиям нахождения в оперативной памяти информационной системы программные закладки делятся на [27]:

- резидентные закладки, постоянно находящиеся в оперативной памяти до перезагрузки или завершения функционирования информационной системы;
- нерезидентные закладки, выгружающиеся из оперативной памяти информационной системы по истечении определенного времени, либо при выполнении определенных условий.

3.4 Аппаратные закладки

Аппаратная закладка – устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных средств информационной системы. Результатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение ее нормального функционирования, например несанкционированный доступ к информации, ее изменение или блокирование [29].

Также аппаратной закладкой может называться отдельная микросхема, несанкционированно подключаемая к атакуемой системе для достижения тех же целей [29].

Аппаратные закладки можно классифицировать по различным основаниям, следующим образом – рис. 9 [30].

1. По типу:

- функциональная – закладка производится путем изменения состава аппаратных средств, добавлением или удалением необходимых элементов (например, транзисторов или логических вентилей в микросхеме);
- параметрическая – закладка производится путем использования уже существующих компонентов аппаратного средства.

2. По расположению закладки:

- в виде элементов микросхемы;
- в отдельной микросхеме;
- на электронной плате;
- в аппаратных средствах информационной системы;
- пространственно-распределенная по нескольким аппаратным средствам.

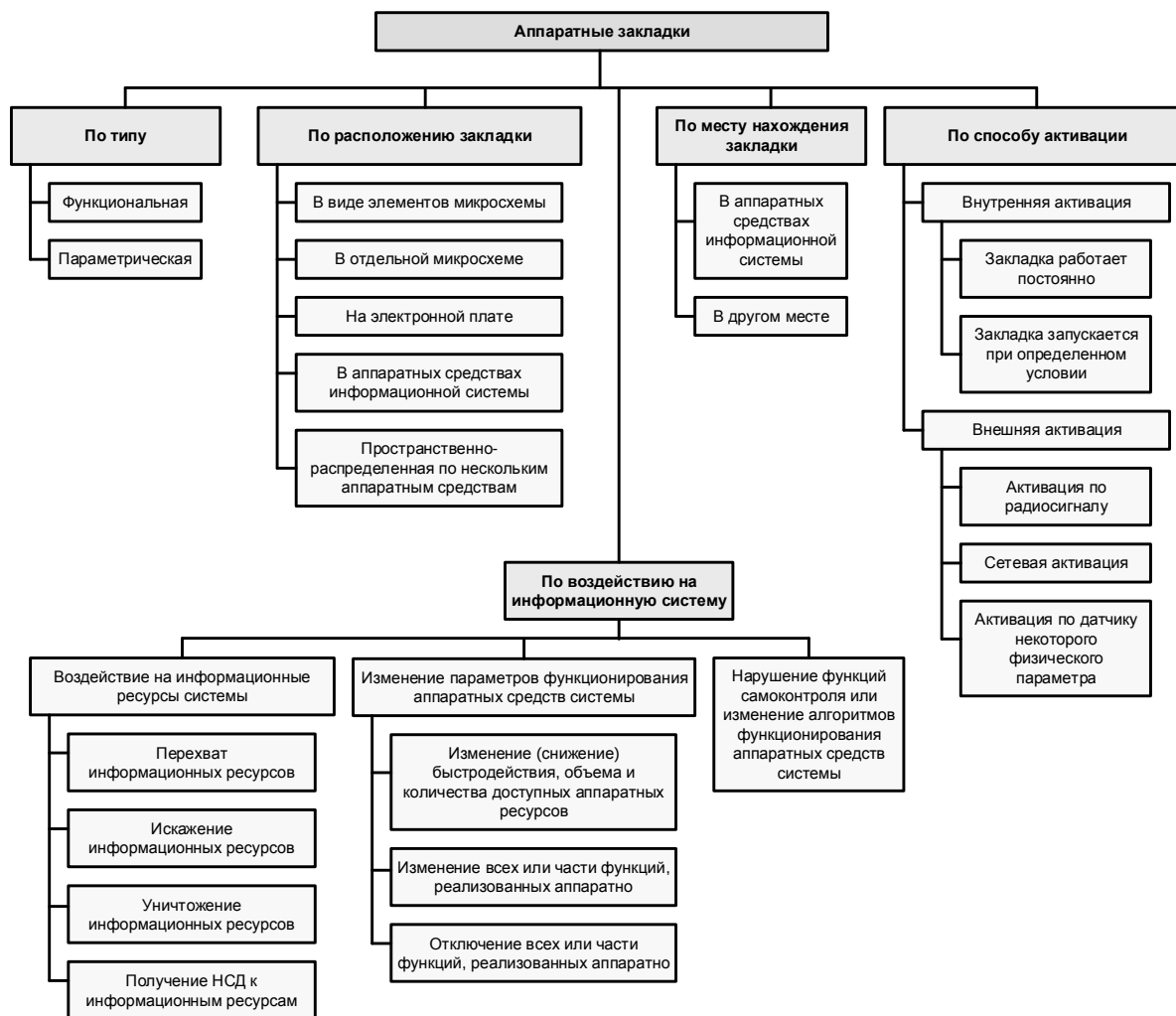


Рис. 9. Классификация аппаратных закладок

3. По объему – характеризует количество измененных, добавленных или удаленных элементов аппаратных средств, необходимых для внедрения закладки.
4. По месту нахождения закладки относительно ассоциированной информационной системы:
 - в аппаратных средствах информационной системы;
 - в другом месте.
5. По способу активации:
 - внутренняя активация:
 - закладка работает постоянно в составе аппаратного средства;
 - закладка запускается при определенном условии, заложенном при ее разработке;
 - внешняя активация – для запуска закладки используется внешний сигнал, который принимается антенной или датчиком:
 - активация по радиосигналу;
 - сетевая активация;
 - активация по датчику некоторого физического параметра.
6. По воздействию на информационную систему:
 - воздействие на информационные ресурсы системы:

- перехват информационных ресурсов;
- искажение информационных ресурсов;
- уничтожение информационных ресурсов;
- получение несанкционированного доступа к информационным ресурсам;
- нарушение функций самоконтроля или изменение алгоритмов функционирования аппаратных средств системы;
- изменение параметров функционирования аппаратных средств системы:
 - изменение (снижение) быстродействия, объема и количества доступных аппаратных ресурсов;
 - изменение всех или части функций, реализованных аппаратно;
 - отключение всех или части функций, реализованных аппаратно.

Схематическая сложность современного микроэлектронного оборудования, тенденции по миниатюризации его элементов ведут к тому, что производители оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, а при подключении устройств к глобальной сети – осуществлять обновление алгоритма их функционирования, а также условий срабатывания.

Краткая характеристика технологий современных аппаратных закладок представлена в таблице 1 [31].

Таблица 1 – Технологии современных аппаратных закладок [31]

Методы внедрения	Методы обнаружения	Методы маскировки
Встраивание закладок в технологию микроядра управления в современных СБИС, построенного на уникальном списке команд (управление основной работой и блокировка и замена неисправных узлов для продления срока службы СБИС)	Технологии послойного сканирования кристаллов	Механизм технологической защиты топологии кристалла от послойного сканирования (впервые внедрен в i486).
	Вычитывание и дизассемблирование аппаратно доступных микрокодов	Размещение микроядер с закладками и ресурсов памяти в области, не доступной пользователю.
Виртуализация вычислений	Анализ контента проходящих по сети данных	Шифрование (мутирование) участков кода, антитрассировка.
Встраивание целевых микроядер и узлов, реализующих стратегию влияния	Мониторинг аномальной активности платформы. Радио-мониторинг. Электромагнитный контроль.	

Достижения в области разработки и внедрения аппаратных закладок напрямую связаны с научным заделом в области микроэлектроники, а также с мощностями электронной промышленности. В настоящее время такие страны как США, Китай, Япония, в которых функционируют развитые производственные комплексы в области микроэлектронной и микропроцессорной техники, имеют потенциальную возможность встраивания аппаратных закладок в производимые ими на экспорт микроэлектронные компоненты. В дальнейшем это позволит контролировать функционирование подавляющей части АСУ технологическими и критическими процессами, а также средств радиоэлектроники в других странах. При этом в отношении этих стран может быть реализован сценарий мгновенного вывода из строя их критической инфраструктуры за счет одновременного отключения входящих в ее состав микроэлектронных компонентов.

В связи с этим можно выделить следующие риски использования импортных микроэлектронных компонентов при производстве систем управления войсками и оружием [31]:

- встроенная технологическая и схемотехническая избыточность микроэлектронных компонентов, превышающая необходимый уровень для предоставления сервисов по прямому назначению, позволяет внедрять в них недеklarированные функции, в том числе и враждебного характера;
- отсутствие технической документации на топологии микросхем и логику функционирования не позволяет в полной мере провести эффективный технический контроль наличия закладок;
- отсутствие гарантированно подтвержденной надежности микроэлектронных компонентов, а также их стойкости к воздействию электромагнитного оружия, позволит противнику эффективно применять это оружие против систем управления войсками и оружием. При этом противник может создать электромагнитную обстановку, гарантирующую выход из строя им же произведенных микроэлектронных компонентов.

Образцом использования аппаратных закладок является обнародованная Э. Сноуденом информация о закладках Агентства национальной безопасности (АНБ) [32, 33, 34], использующихся для несанкционированного сбора данных в интересах разведывательных служб США. Практически все закладки были реализованы на аппаратном или аппаратно-программном уровне (при внедрении в перепрограммируемую память BIOS). Такое внедрение позволяет обеспечить функционирование закладки даже в случае обновления прошивки устройства или переустановки операционной системы, а кроме того, такая закладка слабо поддается обнаружению [33].

Другим ярким примером использования аппаратной закладки в военном конфликте является факт отключения системы иракской ПВО в военном конфликте в Персидском заливе в 1991 г. Тогда при проведении операции «Буря в пустыне» система ПВО Ирака оказалась заблокированной по неизвестной причине. Несмотря на отсутствие исчерпывающей информации по

этому инциденту, высказывалось предположение, что ЭВМ, входящие в состав системы ПВО, закупленные Ираком у Франции, содержали специальные управляемые «электронные закладки», блокировавшие работу вычислительных систем по внешней команде [27].

Такое действие закладки актуализирует вопросы обеспечения доверенной аппаратной среды при разработке электронных систем для критической инфраструктуры государства. Так как опыт локальных военных конфликтов показывает, что на первых этапах активных военных действий системы управления войсками и оружием, построенные на импортных компонентах, будут выводиться из строя в первую очередь.

При этом в настоящее время фиксируются факты поставки в Вооруженные силы России вычислительной техники, которая фактически произведена иностранным изготовителем, снабжена разнообразными аппаратными закладками (например, одновременно в BIOS-е и сетевой карте компьютера), однако которая, пройдя перемаркировку и установку отечественного программного обеспечения считается де-юре «отечественного производства». При том, такие «отечественные производители», организующие подобные поставки, как правило, не имеют персонала должной квалификации для обнаружения и деактивации встроенных в импортную технику аппаратных закладок, чем создают угрозу обороноспособности страны [35].

3.5 Нейтрализаторы тестовых программ и программ анализа кода

Одним из способов противодействия угрозам программных закладок является проверка программ, используемых в информационных системах управления критической инфраструктуры в процессе сертификационных испытаний и тематических исследований по требованиям безопасности [36, 37].

Сертификационные испытания и тематические исследования проводятся путем [36, 39]:

- функционального тестирования программного обеспечения на соответствие нормативным и методическим документам;
- структурного (статического и динамического) анализа программного обеспечения на отсутствие недеklarированных возможностей.

При этом эксперты в области тестирования могут использовать дополнительные методы и приемы проверки кода, например: инспекция кода, использование статических анализаторов, изучение бюллетеней безопасности, организация стресс-тестирования и др.

При отсутствии исходных текстов программ применяются подходы реверс-инжиниринга и функциональные методы (по принципу «черного ящика»).

Реверс-инжиниринг может проводиться путем [36]:

- ретрансляции/дизассемблирования, прогона в отладочном режиме — для машинных и процедурных языков;
- высококачественной декомпиляцией — для языков с промежуточным кодом.

Сложность и размер современных программ таков, что для проведения сертификации используются специальные тестовые программы и анализаторы кода. Как правило, они ведут динамический анализ программного обеспечения, пока оно выполняется на реальном или виртуальном процессоре, фиксируя трассу управления, и формируемые потоки данных.

При использовании атакующих средств, например, таких как программная закладка, требуется обеспечить ее маскировку. В этом случае используется обеспечивающие средства – нейтрализаторы тестовых программ и программ анализа кода. Цель данных средств – затруднить анализ трассы исполнения программы и скрыть факт наличия закладки.

Средства нейтрализации тестовых программ и программ анализа кода используются либо на этапе компиляции исходного текста в машинный код, либо уже в процессе выполнения программы.

К основным способам нейтрализации тестовых программ относятся (рис. 10) [38, 39, 40]:

- обфускация (запутывание) кода;
- упаковка и шифрование кода;
- определение факта применения тестовых программ и противодействие отладке;
- полиморфизм (сагомодифицирующийся код).



Рис. 10. Классификация способов нейтрализации программ

Рассмотрим данные способы более подробно.

Обфускация кода – приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ и понимание алгоритмов работы, а также модификацию при декомпиляции. Обфускация может осуществляться на различных уровнях: уровне алгоритма, уровне исходного текста, уровне машинного кода (ассемблерного текста). Кроме того, выделяют обфускацию на уровне виртуальных машин. Для создания запутанного машинного кода могут использоваться специализированные компиляторы, использующие неочевидные или недокументированные возможности среды исполнения программы. Существуют также специальные программы, производящие обфускацию, называемые обфускаторами [39].

Недостатками обфускации кода являются:

- код после обфускации может стать более зависимым от используемой платформы или компилятора;

- после обфускации дальнейшая отладка и тестирование программного кода становится невозможна;
- обфускация обеспечивает скрывание программных закладок через неясность программного кода, однако ни один из существующих обфускаторов не гарантирует устойчивости к определенному уровню сложности декомпиляции и не обеспечивает безопасности на уровне современных криптографических схем.

Упаковка и шифрование участков кода. При этом способе в программное обеспечение встраивается код шифратора и генератор ключей, после чего программа в процессе работы «на лету» дешифрует инструкции машинного кода и передает их на исполнение. Использование такого способа противодействия тестовым программам позволяет существенно сузить их возможности по тестированию. Данный подход делает невозможным непосредственное дизассемблирование кода программы. Помимо этого, сохранение дампов памяти для последующего дизассемблирования становится крайне неэффективным, т.к. каждый дамп содержит только небольшой расшифрованный фрагмент программы [39].

Определение факта применения тестовых программ и противодействие отладке. Существует ряд приемов, позволяющих обнаружить выполнение тестирования и отладки. В случае обнаружения этого факта со стороны программы предпринимаются действия, направленные на противодействие исследованию за счет изменения логики своего функционирования:

- меняется работа алгоритмов;
- блокируется исполнение кода программы;
- «портятся» данные отладчика.

Такие способы противодействия отладке преодолеваются применением потактовых симуляторов. В этом случае обнаружение отладки возможно только из-за ошибок в симуляторе, приводящих к отличному от аппаратной платформы поведению [39].

Полиморфизм – генерация различных версий машинного кода для одного и того же алгоритма. Технология полиморфной генерации машинного кода позволяет проводить запутывающие преобразования защищаемого программного обеспечения. Для этого производится встраивание дополнительных или незначущих инструкций в защищаемый код, перестановка последовательности выполнения инструкций. Как правило, на этапе компиляции в программное обеспечение добавляется полиморфный генератор, который в процессе функционирования программы проводит модификацию ее машинного кода [40]:

- перестановка, обмен местами инструкций, порядок следования которых неважен;
- добавление «мусорных команд»;
- введение незначущих переменных;
- изменение процедуры самомодифицирования и др.

3.6 Средства создания ложных объектов информационного пространства

При защите информационных систем большое внимание уделяется вопросам обнаружения и нейтрализации уязвимостей входящего в их состав программного обеспечения (ПО). В настоящее время все основные способы решения данной задачи основываются на применении «стратегии запрета». Для этого в ручном или автоматизированном режиме проводится поиск уязвимостей ПО информационной системы, информация о которых имеется в открытых или закрытых базах данных. После обнаружения уязвимость нейтрализуется либо за счет обновления ПО, либо за счет использования средств защиты информации, таких как межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты и т.д., которые делают невозможным эксплуатацию данной уязвимости для реализации несанкционированного доступа [41].

Однако, как показывает практика, такая стратегия оказывается неэффективной против уязвимостей «нулевого дня». Это связано с тем, что между выпуском ПО и появлением информации об уязвимости, а тем более устранением ее разработчиками, в большинстве случаев проходит большое количество времени, в течение которого система оказывается уязвимой. Несмотря на то, что правильно настроенные средства защиты информации делают эксплуатацию некоторых из таких уязвимостей невозможной, всегда остается вероятность наличия не устраненных уязвимостей, а также уязвимостей в ПО самих средств защиты [41].

В связи с этим в настоящее время актуальным становится применение «стратегии обмана» или отвлечения атаки информационного оружия на ложный информационный ресурс. Как показали исследования [42], реализуя «стратегию обмана» атакующей системы и отвлекая атаку на ложный информационный ресурс, можно не только не позволить получить несанкционированный доступ к защищаемой информации, но и провести ответную информационную атаку – дезинформировав атакующую сторону. Кроме того, в период отвлечения атаки на ложные информационные ресурсы возможен сбор данных об атакующей стороне для компрометации последней.

В общем случае можно выделить два типа ложных ресурсов, ориентированных на различные сферы информационного противоборства:

- ложные объекты и ресурсы в семантической части информационного пространства (например, дезинформация или заведомо ложная информация, размещаемая в СМИ и в сети Интернет);
- ложные объекты и ресурсы в телекоммуникационной части информационного пространства (например, ложные сети, узлы, БД и т.д.).

Ложные объекты и ресурсы, размещаемые в семантической части информационного пространства, ориентированы на ведение информационного противоборства в психологической сфере и направлены, главным образом, на обеспечение информационно-психологических операций.

Ложные объекты и ресурсы в телекоммуникационной части информационного пространства ориентированы на ведение информационного противоборства в технической сфере. Они предназначены для обмана и отвлечения на себя атакующих информационно-технических воздействий.

К ложным объектам и ресурсам в телекоммуникационной части информационного пространства, на которые возможно эффективное отвлечение проводимых противником атак, можно отнести:

- узлы телекоммуникационных сетей;
- вычислительные и информационно-управляющие системы;
- операционные системы;
- прикладное программное обеспечение;
- базы данных и системы управления ими;
- программы управления контентом сайтов, новостных агрегаторов, страниц во внутренней сети или в сети Интернет.



Рис. 11. Классификация ложных объектов информационного пространства

В качестве средств создания и использования ложных объектов в телекоммуникационной части информационного пространства можно рассматривать программное обеспечение на основе технологий виртуализации. Такие программные средства виртуализации, как VMware ESX/ESXi, Microsoft Hyper-V, Citrix Xen Server и др., позволят создать виртуальную инфраструктуру, наполнить ее ложными объектами, содержащими дезинформацию и впоследствии управлять такой системой [41].

Кроме вышеуказанных средств виртуализации возможно использование других способов и средств создания ложных объектов. К ним можно отнести – создание ложных сетей путем подмены адресов объектов сети, развертывания дополнительных сетей с организацией по ним дезинформирующего информационного обмена, использование в сети средств защиты со специально введенными в них уязвимостями (так называемых «приманок»). С примерами

подобных решений можно ознакомиться в работах отечественных специалистов [60, 61, 62].

3.7 Средства моделирования боевых действий

Анализ вооруженных конфликтов свидетельствует о том, что успех сопутствует стороне, проявляющей большую активность и инициативу, эффективно управляющей подчиненными силами и средствами. Эволюционный путь развития автоматизированных средств управления войсками и оружием привел к разработке и принятию концепции создания системы моделирования военных действий [43].

В связи с развитием современных супер-компьютерных технологий уже в ближайшее время можно ожидать появления достаточных вычислительных возможностей для моделирования боевых действий с приемлемой степенью адекватности. Средства такого моделирования основаны на манипулировании информацией о составе, формах и способах действий войск (сил). Использование средств моделирования боевых действий позволят точно выбрать оптимальную стратегию действий при заданном составе группировки своих сил и средств, выбрать оптимальную траекторию развития противоборства с учетом вероятных действий противника и тем самым обеспечит подавляющее асимметричное информационное превосходство над противником, при условии отсутствия у него подобных средств. При противоборстве двух сторон, обладающих подобными средствами, может создаться ситуация, что конфликт закончится еще в угрожаемый период. Когда сторона, которая по результатам моделирования не сможет найти выигрышной стратегии, самостоятельно признает себя проигравшей.

Вышеуказанные факты, а именно – использование средств моделирования боевых действий для достижения информационного превосходства над противником за счет обработки информации, позволяет отнести данные средства к информационному оружию.

Начиная с 70-х годов моделирование становится обязательным инструментом военных исследований. Широкое развитие получают имитационные модели, которые находят применение в военном планировании. В 80-е годы модели становятся повседневным рабочим инструментом в военном планировании, в непосредственном обеспечении деятельности руководства Вооруженных сил (ВС). Унифицируется информационное обеспечение моделей (базы данных). Проектируются иерархические системы моделей боевых действий различного уровня. Все более широкое распространение получает использование моделей в АСУ военного назначения. В ходе учений ACE-89 в Германии впервые реально была задействована система, объединившая модели различных уровней (DWS - Distributed Wargaming System). 90-е годы характеризуются еще более масштабными проектами внедрения моделирования в повседневную деятельность с охватом всех видов ВС США. Были созданы органы, обеспечивающие централизованное руководство разработкой и применением моделирования МО

США, координацию соответствующих работ как между видами ВС, так и в рамках какого-либо одного из направлений применения моделирования. Совершенствование средств имитации и моделирования в этот период ведется по пути интеграции моделей между собой и с состоящими на вооружении ВВТ, а также в направлении увеличения числа военнослужащих, выполняющих учебно-боевые задачи с использованием тренажерных комплексов. Значительно возросло количество учений различного уровня с использованием автоматизированных систем моделирования боевой обстановки. С середины 90-х годов командование американских ВС начало использовать новую форму проведения маневров – компьютерные учения с ограниченным привлечением войск и штатного ВВТ [45].

С начала 2000-х годов Пентагон при формировании военно-технической политики включил средства имитации и моделирования боевых действий в число приоритетных технологий. С начала 2000-х годов военное руководство США выделяет средства имитации и моделирования боевых действий в число приоритетных технологий при формировании военно-технической политики. Высокая динамика развития вычислительной техники, технологий программирования, системотехнических основ моделирования различных реальных процессов обозначили огромный прорыв США в области разработки моделей и имитационных систем [44, 45].

В настоящее время в министерстве обороны США действует классификация, определяющая назначение модели, объекты и процессы, метод моделирования (рис. 12) [45].

По назначению американские специалисты также выделяют три группы моделей [45]:

- используемые в целях анализа и оценки (обеспечение оперативной работы);
- применяемые в сфере создания ВВТ;
- предназначенные для обучения личного состава, обеспечения боевой подготовки войск и штабов.

В последнее время в ряде официальных документов военного ведомства предлагается более подробное подразделение моделей с выделением семи функциональных сфер моделирования [45]:

- оценка эффективности действий формирований в самостоятельных, совместных и объединенных операциях видов и родов сил;
- доктринальные исследования (военно-научные исследования и разработка концепций в области строительства ВС и их боевого применения);
- боевое обеспечение или поддержка операций (разведка, РЭБ и др.);
- создание ВВТ (снижение стоимости новых образцов и сокращение времени их создания, включая сферу НИОКР и закупок);
- испытания и оценка (потребностей ВС, повышение качества принимаемых решений в сфере планирования и разработки бюджетных программ, оценка эффективности новых образцов ВВТ);
- тыловое обеспечение;

- боевая подготовка и обучение личного состава.

При этом в последнее время акцент делается на создание систем моделирования, направленных на решение задач в области строительства и применения объединенных и коалиционных группировок войск (сил).

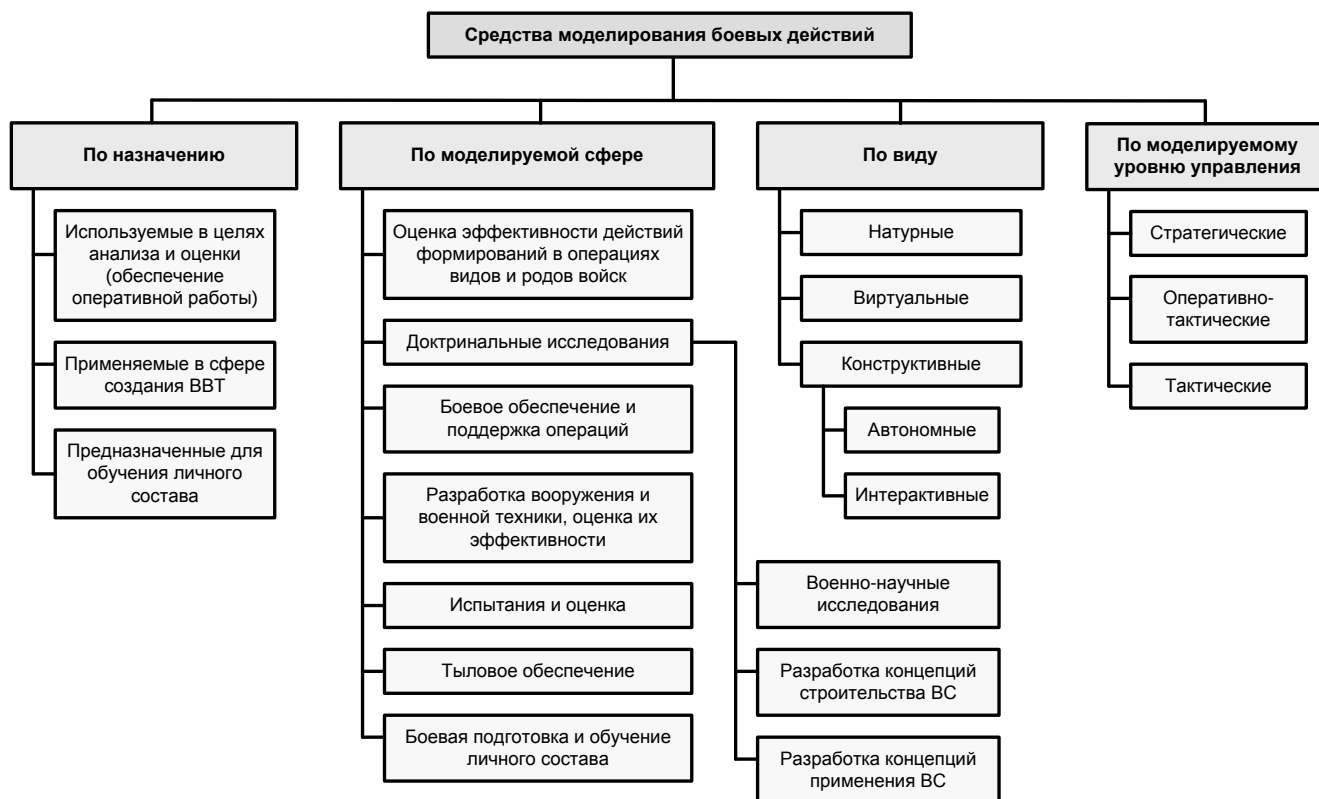


Рис. 12. Классификация средств моделирования боевых действий

Научно-технический совет МО США с начала 90-х годов ввел свой вариант классификации моделей, выделив три основные их вида, подчеркивая различие в степени и характере участия человека в процессе моделирования [45]:

- натурные;
- виртуальные;
- конструктивные.

К натурным системам относятся традиционные войсковые и командно-штабные учения с привлечением штатной техники и личного состава. В настоящее время отмечается тенденция к сокращению масштабов натурального моделирования и, напротив, расширяется использование других видов моделирования и имитации, особенно это касается виртуальных систем [45].

Виртуальные системы представляют собой человеко-машинные системы, в которых совмещается натурное и компьютерное моделирование. В первую очередь – это различные тренажеры ВВТ, применяемые для обучения. В настоящее время в большинстве виртуальных систем некоторые из компонент представлены в натурном виде, например реальными образцами вооружения и военной техники, а также обслуживающим их персоналом. В качестве весьма

перспективной разновидности виртуальной имитирующей системы может рассматриваться концепция так называемого виртуального прототипа. В таких системах предполагается полная замена реального оборудования его компьютерной имитацией. Данный подход широко используется при создании систем ВВТ [45].

Конструктивные системы могут быть [45]:

- полностью автономными (процесс моделирования не требует участия человека),
- интерактивными человеко-машинными системами.

Большинство используемых моделей являются именно конструктивными. Здесь предметная область, характерные для нее объекты и процессы представляются с помощью математического (алгоритмического) описания и соответствующего программного обеспечения. Термин применяется главным образом, чтобы подчеркнуть отличие этого класса моделей от натуральных и так называемых виртуальных моделей. К конструктивным системам относятся разного рода имитационные модели [45].

Архитектура современных систем моделирования боевых действий стандартизирована. Она включает библиотеки стандартных программных модулей – генерирования случайных чисел, форматирования специфических докладов, выполнения сложных математических вычислений, управления ходом моделирования и др. [45].

Продолжаются работы по развитию объектно-ориентированной архитектуры моделей, призванной обеспечить более эффективное взаимодействие моделей и их использование. Такая архитектура позволяет создать инфраструктуру моделирования, которая может быть многократно использована в рамках разработки множества проектов создания моделей. При этом потребуется лишь добавить новую функциональность, реализующую решение новой задачи (описание новой среды функционирования или концептуальной схемы реального мира). По расчетам американских специалистов в этой области, возможно сокращение времени разработки моделей на 90% [45].

Важным направлением деятельности Министерства обороны США в сфере военного моделирования является оценка, подтверждение и сертификация моделей. Данные процедуры предполагают установление степени соответствия моделей процессам реального мира, а также установление применимости модели для решения специфических задач. Тем самым очерчиваются круг проблем или специфические условия существования проблем, для решения которых применима данная модель [45].

Основные направления модернизации объединенных систем моделирования и имитации боевых действий связаны в первую очередь с необходимостью создания новых моделей, а также с совершенствованием существующих систем. Дефицит моделей, вызванный динамизмом и глобальностью изменений в мире, а также появлением новых предметных областей, в значительной степени преодолен за последние годы. Тем не менее актуализация исследований применения ВС США в локальных конфликтах и в

различного рода «невоенных» операциях, например, при осуществлении миротворчества в борьбе с терроризмом, наркобизнесом и т. п., требуют разработки таких моделей, в которых был бы отражен значительно расширившийся спектр возможного применения Вооруженных сил. Требуются новые или уточненные модели для использования в следующих предметных областях: системы управления и связи; вычислительные системы и разведка; применение систем ПРО; радиоэлектронная борьба; применение оружия нелетального воздействия; роботизированные комплексы и системы; специальные операции; миротворческие операции; борьба с терроризмом и наркобизнесом и другие [45].

Высказывается мнение, что для нового поколения моделей требуется более полный учет взаимодействия многих военных, политических, экономических, этнических, религиозных и некоторых иных факторов, так или иначе влияющих на глобальную и региональную безопасность в современных условиях [45].

Перспективы развития моделирования связываются с развитием таких ключевых направлений развития науки и технологий, как: высокопроизводительные вычисления; компьютерные сети; визуализация; системы виртуальной реальности; распределенные системы моделирования. Благодаря программе Министерства обороны США по высокопроизводительным вычислениям ресурсы суперкомпьютеров становятся все более доступными для имитации через облачные вычислительные ресурсы [45].

В целом необходимо отметить, что развитие систем моделирования и имитации в США рассматривается как один из основных факторов обеспечения эффективности строительства и применения Вооруженных сил. Громадный потенциал, накопленный в данной области, уже сейчас оценивается как значительно опережающий возможности других стран мира в этой сфере [44].

В перспективе ожидается дальнейшее глобальное комплексирование моделей и внедрение систем виртуальной реальности (искусственного многомерного боевого пространства) на базе телекоммуникационных сетей, призванных обеспечить доступ пользователей как к оперативной, так и к физической моделируемой среде, к стандартизированным моделям и базам данных, а также к различного рода сценариям. Перспективные системы моделирования боевых действий будут имитировать применение вооруженных сил на любом континенте, на море, в воздухе и космическом пространстве, весь спектр их задействования (включая миротворческие операции, борьбу с терроризмом и т. п.). В будущем такие системы смогут с высокой степенью адекватности моделировать действия на фоне искусственно созданной боевой обстановки, воспроизводящей особенности любого театра военных действий (ТВД). А в качестве противника будут выступать как полностью, так и частично компьютеризированные «аналоги» реальных войсковых формирований [44].

Более подробная информация о подходах к моделированию боевых действий представлена в работе [46]. А примеры реальных средств

моделирования боевых применяемых в США в настоящее время – в работах [44, 45]. Кроме того, в работе [43] рассмотрен вариант подобного комплекса, разработанного специалистами республики Беларусь.

3.8 Средства технической разведки

Средства технической разведки предназначены для несанкционированного доступа к информации, ее копирования, а также преодоления подсистем защиты информации у технических и компьютерных систем противника. В связи с этим, с полным основанием их можно отнести к одному из видов обеспечивающего информационно-технического оружия. Средства технической разведки позволяют получить информацию об атакующих средствах информационно-технического 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, связанные с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

Далее кратко рассмотрены средства основных видов технической разведки, при этом более полную информацию по этим средствам можно получить в фундаментальных работах в этой области – [47, 63, 64].

Техническая разведка – целенаправленная деятельность по добыванию с помощью технических средств соответствующих сведений в целях обеспечения военно-политического руководства своевременной информацией по разведываемым странам и их вооруженным силам [47].

Доля технической разведки в общей системе добывания защищаемой информации достаточно велика и, по некоторым оценкам, может составлять до 50% и более. Причем дальнейшее развитие науки и техники объективно приводит к повышению роли и значимости технической разведки [49].

При анализе технических средств разведки используют различные классифицирующие признаки.

1. По месту размещения технические средства разведки подразделяют на:

- космические;
- воздушные;
- наземные;
- кибернетические (размещаемые в информационном киберпространстве).

Для разведки используются различные каналы утечки информации, которые по основанию используемой физической среды (поля) классифицируются на [48, 49]:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (звуковые колебания в звукопроводящей среде);
- электрические каналы (напряжения и токи в токопроводящих коммуникациях);

- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой частях спектра);
- материально-вещественные каналы (бумага, фото, магнитные носители, отходы, выбросы и т.д.);
- другие каналы (радиационные, магнитометрические, сейсмические и т.д.);

2. В соответствии с классификацией каналов утечки информации выделяют следующие *виды технической разведки*, которые используют соответствующие средства [47, 48]:

- радиоэлектронную;
- оптическую;
- оптико-электронную;
- акустическую;
- гидроакустическую;
- химическую;
- радиационную;
- сейсмическую;
- магнитометрическую;
- компьютерную;
- измерительно-сигнатурную.

Классификация средств технических разведок приведена на рис. 13.

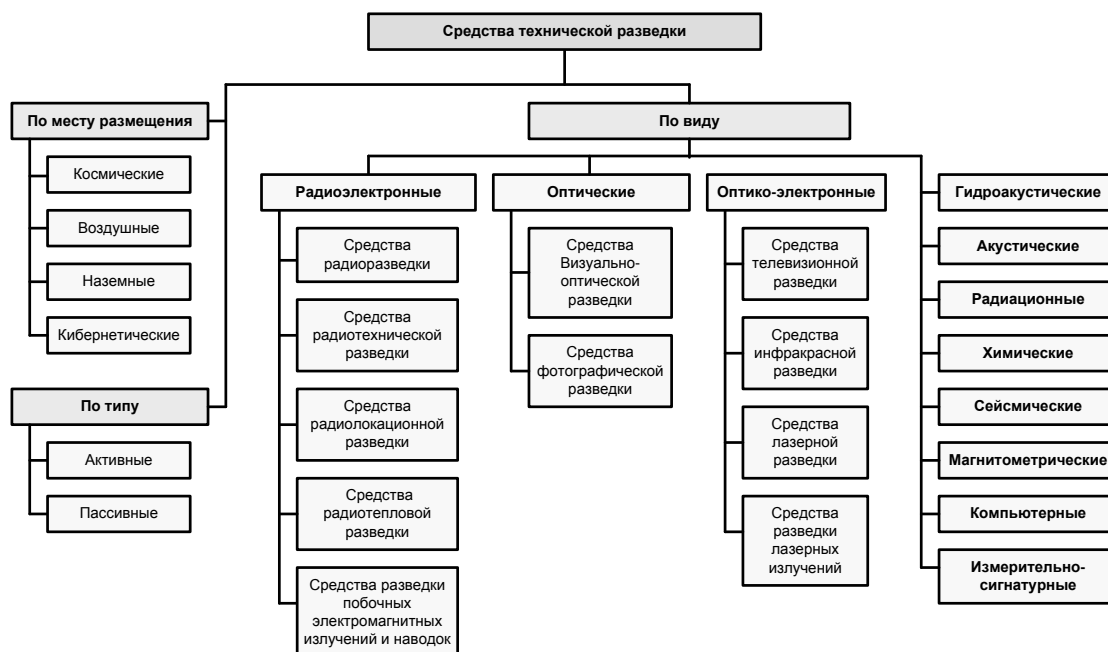


Рис. 13. Классификация средств технической разведки [50]

Рассмотрим данные виды разведок и соответствующие им технические средства более подробно на основании материала, представленного в работах [47, 63, 64].

Радиоэлектронная разведка (РЭР) – это процесс получения информации в результате приема и анализа электромагнитных излучений (ЭМИ) радиодиапазона, создаваемых работающими РЭС [47].

ЭМИ, создаваемые объектами разведки, могут быть первичными (собственными) или вторичными (отраженными) [47].

РЭР позволяет решать следующие задачи [47]:

- обнаруживать объекты, определять их местоположение и параметры движения;
- определять параметры объектов и характер их изменения во времени;
- определять назначение объектов и их типы;
- перехватывать передаваемую по каналам связи информацию.

Средства РЭР работают в пассивном или активном режиме (без излучения электромагнитных волн или с излучением) в широком диапазоне спектра радиочастот [47].

Радиоэлектронная разведка, в зависимости от ее целевого назначения, подразделяется на стратегическую и тактическую.

Стратегическая РЭР ведется в интересах правительственных органов и высшего военного командования с целью добывания всесторонней информации о разведываемой стране через его радиоэлектронные средства. Такая информация необходима для подготовки вооруженных сил и ресурсов страны к войне, принятия решения о начале военных действий и умелого ведения стратегических операций [47].

Тактическая РЭР считается одним из основных видов обеспечения войск информацией путем непрерывного слежения за электромагнитным излучением многочисленных военных устройств и систем противника. Она в состоянии добывать важные сведения для ведения боевых действий силами соединений, частей и подразделений [47].

Различают наземную, морскую, воздушную и космическую радиоэлектронную разведку. По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.

Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся [47]:

- открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи;
- тактико-технические данные и особенности разведываемых активных радиоэлектронных систем (частота настройки, вид модуляции и манипуляции, диаграммы направленности антенн, мощность излучения и т.п.), составляющие их «электронный почерк»;
- типы радиоэлектронных систем: радиосвязи, радиолокации, радионавигации, наведения ракет и дальнего обнаружения, различные телеметрические системы передачи данных;
- количество обнаруживаемых радиоэлектронных систем противника;
- местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемых разведываемой стороной впервые. Целью добывания технической информации является своевременная разработка

аппаратуры и методов радиоэлектронной разведки новых систем оружия и средств управления противника [47].

Для получения такой информации средствами РЭР ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками. При этом к наиболее важным источникам РЭР относятся:

- активные средства радиосвязи, используемые во всех видах вооруженных сил и в интересах управления государством;
- радиолокационные станции (РЛС) разных типов и назначений, применяемые, главным образом, в ПВО;
- автоматизированные системы управления, слежения и наведения ракетного и противоракетного оружия, а также космических объектов;
- радионавигационные системы, используемые в морской, воздушной и космической навигации;
- различные телеметрические системы передачи информации.

Радиоэлектронная разведка включает в себя следующие составные части [47]:

- радиоразведка;
- радиотехническая разведка;
- радиолокационная разведка;
- радиотепловая разведка;
- разведка побочных электромагнитных излучений и наводок.

Радиоразведка – самый старый вид радиоэлектронной разведки. Она ориентирована против различных видов радиосвязи. Основное содержание радиоразведки – обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций; пеленгование их сигналов; анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения; снижение нагрузки или подрыв криптографических систем [47].

Сведения радиоразведки о неприятельских станциях, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления, место размещения баз и стартовых площадок ракетного оружия и др.

Радиотехническая разведка (РТР) – вид разведывательной деятельности, целью которого является сбор и обработка информации, получаемой с помощью радиоэлектронных средств о радиоэлектронных системах по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах, смысловом содержании сигналов. Объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоуправления, радиотелекодовые системы, а также

ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т. п.) [47].

Средства РТР устанавливаются на самолетах, спутниках, кораблях, других объектах.

Радиолокационная разведка (РЛР) – вид технической разведки, в ходе которой информация добывается с помощью радиолокационных станций. РЛС могут быть стационарные наземные, переносные и установленные на самолетах, спутниках, кораблях, других мобильных объектах [47].

Радиотепловая разведка – вид разведывательной деятельности, целью которой является сбор информации о местоположении наземных, морских, воздушных и космических объектов по их тепловому излучению в радиодиапазоне. Характеристики радиотеплового излучения, такие как интенсивность и спектральный состав, зависят от физических свойств вещества и температуры объекта. Разведка ведется с помощью радиотеплолокационных станций, устанавливаемых на воздушных и космических платформах. Радиотепловая разведка возможна только при наличии контрастности теплового излучения объектов и фона (земной поверхности, неба и т.д.) [47].

Разведка побочных электромагнитных излучений и наводок – получение информации о передаваемой, обрабатываемой информации, а также информации об особенностях построения и функционирования технических средств путем анализа их побочных электромагнитных излучений и наводок от них.

Оптическая разведка – добывание информации с помощью оптических средств, обеспечивающих прием электромагнитных колебаний ультрафиолетового, видимого и инфракрасного диапазонов, излученных или отраженных объектами и предметами окружающей местности [47].

Оптическая разведка подразделяется на [47]:

- визуально-оптическую разведку;
- фотографическую разведку.

Оптико-электронная разведка (ОЭР) – процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и инфракрасного диапазонов, излученных или отраженных объектами и местностью [47].

ОЭР подразделяют на [47]:

- телевизионную разведку;
- инфракрасную разведку;
- лазерную разведку;
- разведку лазерных излучений.

Средства ОЭР устанавливаются на космических и воздушных носителях, а также могут применяться в наземных условиях, например, при ведении технической разведки [47].

Средства ОЭР делятся на [47]:

- пассивные;

- активные.

Пассивные основаны на приеме собственного или переотраженного излучения объектов разведки. Активные предполагают использование для подсвета местности собственного излучателя. Зондирующее излучение рассеивается объектами, местными предметами и местностью, часть этого излучения поступает на вход оптической системы аппаратуры разведки с последующим его преобразованием, обработкой и индикацией на соответствующих устройствах [47].

Средства пассивной ОЭР подразделяются на: телевизионные, инфракрасные и средства разведки лазерных излучений. Аппаратура телевизионной разведки охватывает устройства на ЭЛТ и на ПЗС. К средствам инфракрасной разведки относят тепловизоры, тепепеленгаторы, радиометры и приборы ночного видения. Средства разведки лазерных излучений предназначены для обнаружения, определения местоположения и распознавания средств вооружения и военной техники, в состав которых входят лазерные излучатели [47].

Средства активной ОЭР подразделяются на [47]:

- лазерные со сканированием зондирующего светового луча;
- инфракрасные с использованием ИК-излучателя для подсвета местности.

Гидроакустическая разведка – получение информации путем приема и анализа акустических сигналов инфразвукового, звукового и ультразвукового диапазонов, распространяющихся в водной среде от надводных и подводных объектов [47].

По принципу использования энергии акустического излучения средства гидроакустической разведки делятся на активные (гидролокаторы) и пассивные [47].

Активные средства работают по принципу излучения в водной среде зондирующих акустических сигналов с последующим приемом и анализом отраженных от объектов и морского дна эхосигналов [47].

При ведении пассивной гидроакустической разведки используют шумопеленгаторы, которые принимают и анализируют шумовые акустические излучения в водной среде, возникающие при работе двигателей, гребных валов, машин и механизмов различных агрегатов надводных кораблей, подводных лодок и других плавсредств, а также средства разведки, предназначенные для приема и анализа акустических сигналов, создаваемых гидролокаторами, эхолотами, системами гидроакустической связи и др. [47]

Акустическая разведка – получение информации путем приема и анализа акустических сигналов инфразвукового, звукового, ультразвукового диапазонов, распространяющихся в воздушной среде от объектов разведки. Акустическая разведка обеспечивает получение информации, содержащейся непосредственно в произносимой либо воспроизводимой речи (акустическая речевая разведка), а также в параметрах акустических сигналов, сопутствующих работе вооружения и военной техники, механических

устройств оргтехники и других технических систем (акустическая сигнальная разведка) [47].

Радиационная разведка – получение информации в результате анализа радиоактивных излучений, связанных с выбросами и отходами атомного производства, хранением и транспортировкой расщепляющихся материалов, ядерных зарядов и боеприпасов, производством и эксплуатацией реакторов, двигателей и радиоактивным заражением местности [47].

Химическая разведка – добывание информации путем контактного или дистанционного анализа изменений химических свойств состава окружающей среды под воздействием выбросов и отходов производства, работы двигателей, в результате взрывов и выстрелов, преднамеренного рассеивания химических веществ, испытаний и применений химического оружия [47].

Сейсмическая разведка – добывание информации путем обнаружения и анализа деформационных и сдвиговых полей в земной поверхности, возникающих под воздействием различных взрывов [47].

Магнитометрическая разведка – добывание информации путем обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой [47].

Измерительно-сигнатурная разведка ведется в интересах обеспечения успеха военных операций вооруженных сил, создания новых поколений вооружения и военной техники, определения направлений модернизации вооруженных сил, контроля за распространением оружия, окружающей средой, а также выполнением военных договоров [47].

Сущность измерительно-сигнатурной разведки заключается в комплексном характере сбора разведывательной информации: во-первых, измерение геометрических размеров и соотношений статических, динамических и других физических характеристик разведываемых объектов (стационарных и подвижных) и, во-вторых, регистрация сигнатур характерных физических полей, создаваемых этими объектами (электромагнитных, магнитных, радиационных, акустических, сейсмических и других), а также выявление химических и биологических агентов и даже состава конструкционных материалов объектов и их элементов. При этом, используются все существующие датчики: оптические, радиолокационные, лазерные, радиочастотные, акустические, сейсмические, радиационные, химические, оптико-электронной и радиолокационной съемки с перекрытием практически всего спектра электромагнитных колебаний [47].

Следует иметь в виду, что физические измерения и снятие сигнатур не являются самоцелью измерительно-сигнатурной разведки. Главное в ней – выявление назначения, тактики применения, возможностей и основных характеристик, а также уязвимых мест разведываемого объекта [47].

Дополнительные сведения о средствах технической разведки, а также примеры конкретных технических устройств представлены в работах [47, 48, 63, 64].

3.9 Средства компьютерной разведки

Средства компьютерной разведки являются одним из видов средств технической разведки.

Под компьютерной разведкой традиционно было принято понимать получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования [47]. Однако, в настоящее время стало общепризнанным, что это слишком узкий, упрощенный подход к компьютерной разведке и в настоящее время данное понятие активно модернизируется и развивается.

Объектами компьютерной разведки являются компьютерные системы и сети, которые включают: отдельные ЭВМ, многопроцессорные ЭВМ и компьютерные системы, информационно-вычислительные сети, программно-аппаратные комплексы, программное обеспечение ЭВМ, периферийное компьютерное оборудование, различное оборудование, содержащее встроенные процессоры и микро-компьютеры и т.п. [51].

Таким образом, в наиболее общем случае под компьютерной разведкой понимается добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей. В связи с этим, выделяют три типа источников информации для компьютерной разведки [51]:

- данные, сведения и информация, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- характеристики программных, аппаратных и программно-аппаратных комплексов;
- характеристики пользователей компьютерных систем и сетей.

Классификацию средств и способов компьютерной разведки можно провести по нескольким основаниям (рис. 14).

По виду реализации средства компьютерной разведки можно разделить на:

- *физические* – реализованные в виде физических или аппаратных средств, которые подключаются к инфокоммуникационной инфраструктуре, ведут анализ физических полей, побочных электромагнитных излучений и наводок (ПЭМИН) в интересах добывания данных, сведений и информации;
- *программные* – реализованные в виде программных средств, которые в виде вирусов, закладок или специализированного программного обеспечения добывают данные, сведения и информацию за счет анализа логики построения и функционирования компьютерных систем, а также информационных потоков циркулирующей в них.

По принципам построения средств и их функциональному предназначению можно выделить следующие типы компьютерной разведки [51]:

- *семантическая* – обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа

- структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;
- *алгоритмическая* – с использованием программно-аппаратных закладок и недеklarированных возможностей, обеспечивающая добывание данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недеklarированных возможностей компьютерных систем и сетей;
 - *вирусная* – обеспечивающая добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и в системы для перехвата управления компьютерными системами;
 - *разграничительная* – обеспечивающая добывание информации из отдельных компьютерных систем, возможно и не входящих в состав сети, на основе преодоления средств разграничения доступа, а также реализация несанкционированного доступа при физическом доступе к компьютерам, сетям или к компьютерным носителям информации;
 - *сетевая* – обеспечивающая добывание данных из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий;
 - *поточковая* – обеспечивающая добывание информации и данных путем перехвата, обработки и анализа сетевого трафика и выявления структур компьютерных сетей, а также их технических параметров;
 - *аппаратная* – обеспечивающая добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки;
 - *форматная* – обеспечивающая добывание информации и сведений путем «вертикальной» обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем – в информацию для последующего ее наилучшего представления пользователям;
 - *пользовательская* – обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем

обеспечения им доступа к информации, циркулирующей в специально созданной ложной информационной инфраструктуре.

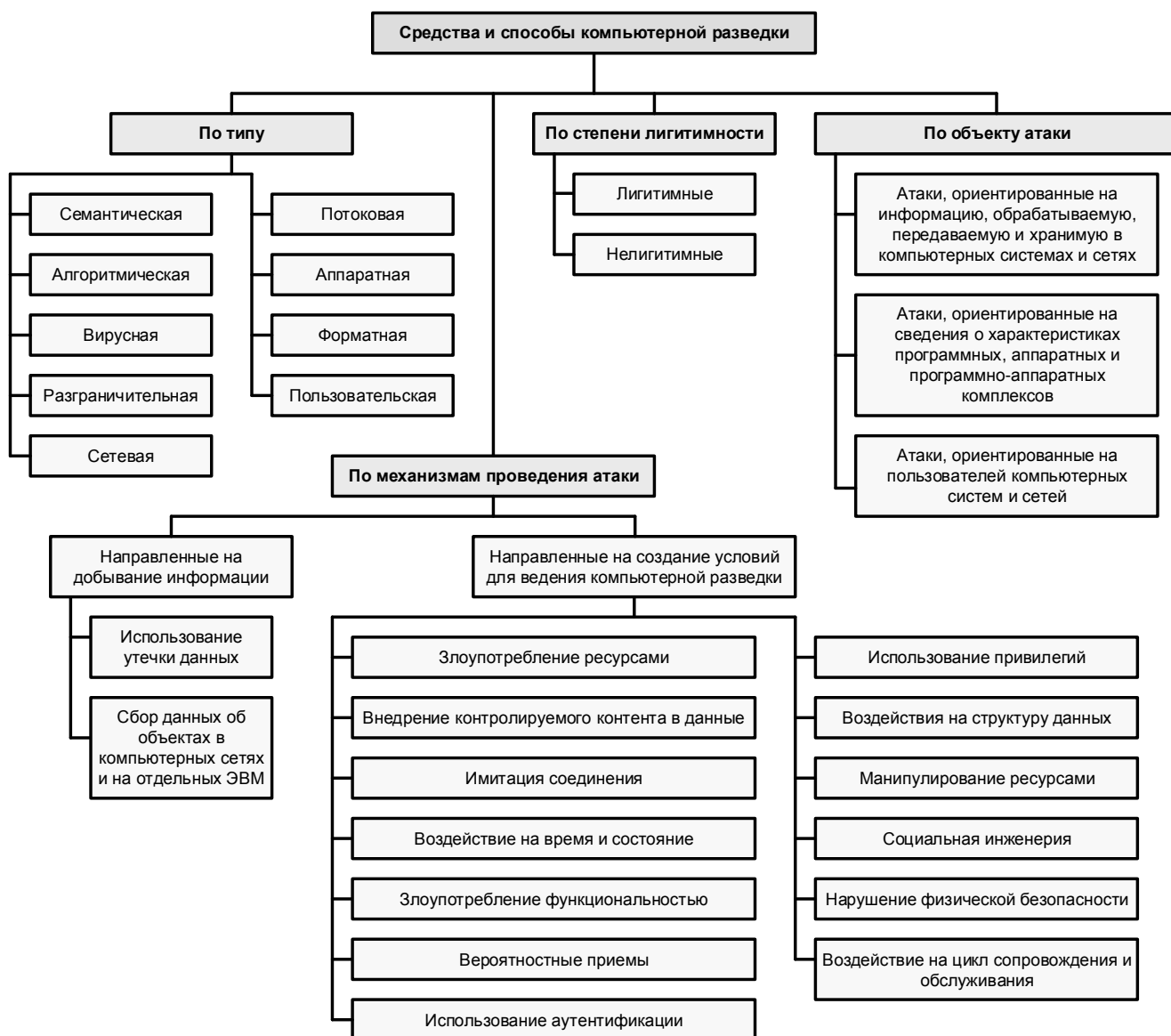


Рис. 14. Классификация средств и способов компьютерной разведки

На данном этапе развития компьютерных систем и сетей эти девять типов компьютерной разведки охватывают все существующие многоуровневые «горизонтальные» и «вертикальные» каналы утечки информации из компьютерных систем и сетей. При этом внутри указанных типов возможно выделение нескольких подтипов разведки, например, по виду добываемой информации на: фактографическую («видовую») и параметрическую.

Основным способом реализации разведки является атака средств компьютерной разведки [52, 53].

Под атакой средств компьютерной разведки будем понимать как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия,

направленные на создание условий благоприятствующих добыванию информации.

Атаки средств компьютерной разведки также можно классифицировать по различным основаниям.

По степени легитимности атаки средств компьютерной разведки можно разделить на [52]:

- легитимные (разведка на основе открытых источников, анализ сетевого трафика);
- нелегитимные (перехват трафика, несанкционированный доступ к компьютерным системам и т.д.).

По объекту атаки [51]:

- атаки, ориентированные на данные, сведения и информацию, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- атаки, ориентированные на сведения о характеристиках программных, аппаратных и программно-аппаратных комплексов;
- атаки, ориентированные на сведения о пользователях компьютерных систем и сетей.

По механизмам проведения атаки [53]:

- атаки, направленные на добывание информации в компьютерных сетях и ЭВМ:
 - использование утечки данных;
 - сбор данных об объектах в компьютерных сетях и на отдельных ЭВМ;
- атаки, направленных на создание благоприятных условий для ведения компьютерной разведки:
 - злоупотребление ресурсами;
 - внедрение контролируемого контента в данные;
 - имитация соединения;
 - воздействие на время и состояние;
 - злоупотребление функциональностью;
 - вероятностные приемы;
 - использование аутентификации;
 - использование привилегий;
 - воздействия на структуру данных;
 - манипулирование ресурсами;
 - социальная инженерия;
 - нарушение физической безопасности;
 - воздействие на цикл сопровождения и обслуживания.

Другие аспекты описания атак, такие как способы нападения и используемые уязвимости, также можно рассматривать в качестве оснований для классификации атак компьютерной разведки.

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества признаков. В научной литературе представлены различные классификации,

отличающиеся полнотой учета признаков. Наиболее полный учет признаков реализован в классификации CAPEC [54], разработанной корпорацией MITRE и применяемой для ведения базы данных образцов компьютерных атак в интересах защиты киберпространства США. Однако, классификация атак CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учитывая этот недостаток классификации CAPEC, отечественными специалистами в работе [53] была предложена классификация атак средств компьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 15.

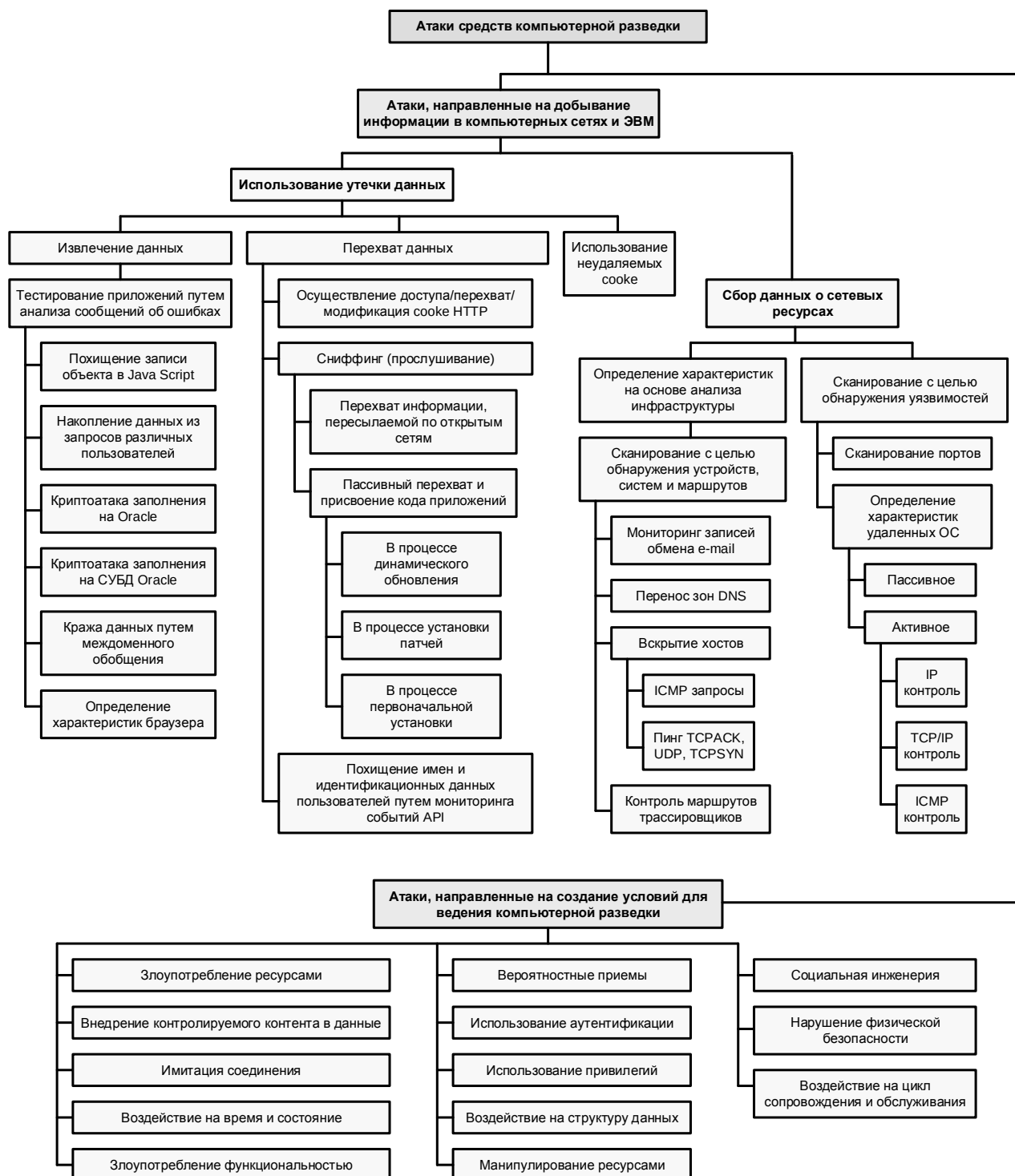


Рис. 15. Классификация атак компьютерной разведки [53]

В настоящее время многие технологически развитые страны активно разрабатывают и совершенствуют собственные средства и комплексы компьютерной разведки. Большинство программ по разработке таких комплексов санкционированы на государственном уровне и ведутся для получения стратегического информационного превосходства в военной, политической и промышленной сфере.

К странам, имеющим наибольшие достижения в области создания глобальных комплексов компьютерной разведки необходимо отнести США (программы: «Carnivore», «Eshelon», «NarusInsight», «Turbulence», «CO-TRAVELER», «PRISM», «Dropmire», «X-Keyscore»), Великобританию (программа «Tempora»), Китай (программа «Золотой щит») и Россию (программа «СОРМ»). Помимо них, другие технически развитые страны также создают свои комплексы компьютерной разведки – Франция (программа «Frenchelon»), Швейцария (программа «Onyx»), Швеция (программа «Titan»), Индия (программы «NATGRID», «Central Monitoring System», «DRDO NETRA»).

3.10 Средства разведки по открытым источникам в глобальном информационном пространстве

Разведка на основе анализа открытых источников информации (Open Source Intelligence – OSINT) является достаточно старым видом деятельности для военной разведки США, и ее история ведется еще со времен Второй мировой войны. Однако, если ранее OSINT рассматривалась как возможность «закрывать информационные бреши» в случае неспособности других видов разведки выполнить поставленную задачу, то сейчас, в связи с развитием в начале XXI века глобального информационного пространства и сети Интернет, по оценкам американского военного руководства, OSINT резко повысила свою значимость [55, 56].

Во многом повышение значимости разведки на основе анализа открытых источников обусловлено тем фактом, что порядка 10-15% необходимой информации имеется в Интернете уже в готовом виде (необходима только ее верификация), а остальные 85-90% информации могут быть получены в результате сравнения, анализа и синтеза разрозненных и разбросанных по разным источникам фактов. Естественно, что информация, полученная таким образом, нуждается в верификации [57].

В сферу интересов такой разведки входит добывание и анализ официальных документов, проектов уставов и наставлений, отслеживание новых научных разработок и проектов, баз данных, коммерческих и государственных интернет-сайтов, сетевых дневников и многого другого [55, 56].

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа. Вариант классификации таких средств представлен на рис. 16.

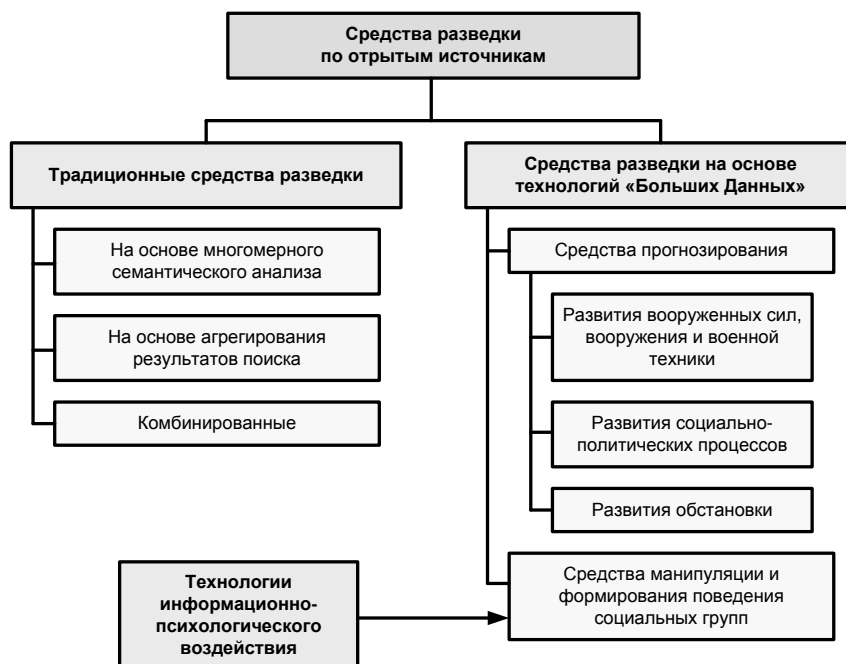


Рис. 16. Вариант классификации средств разведки по отрытым источникам

3.10.1 Средства разведки на основе традиционного семантического анализа и поисковых программ

В качестве средств разведки на основе анализа открытых источников в Интернете традиционно используются специальные программы анализа данных. Под ними понимаются программы-роботы, которые опрашивают сайты и извлекают из них нужную информацию, используя широкий спектр средств лингвистического, семантического и статистического анализа. Действуя автономно, такие программы анализа данных выявляют любую целевую информацию, как только она появится в Интернете [57].

Примерами таких программ могут служить программы «Taiga», «Tropes», «Noemic», «Info Tracer» [57].

В виду того, что имеющимися техническими средствами полностью формализовать процедуру поиска информации пока не представляется возможным, реализовать сложную стратегию поиска необходимой информации часто бывает весьма затруднительно. Поэтому при ведении разведки по открытым источникам в сети Интернет приходится идти по пути информационной избыточности, что накладывает весомые ограничения на релевантность найденных документов. Из-за высокого уровня информационного шума в общем объеме найденных документов значительно увеличивается время, необходимое для аналитической обработки полученных сведений [57].

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию, которая в явном виде находится в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с

совпадающим целевым контентом, начинают «собирать» информационное наполнение запроса пользователей. Более интересным направлением развития средств разведки является анализ разнородных, изначально семантически не связанных между собой, данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направление получило развитие в рамках исследования проблемы «Больших Данных» (Big Data).

3.10.2 Средства разведки на основе технологий «Больших Данных»

Термин «Большие Данные» был впервые введен в 2009 году в специальном выпуске ведущего американского научного журнала Nature, целиком посвященного этой теме. Введение этого понятия обусловлено следующими факторами.

1. Глобальная сеть Интернет перешла в фазу явно выраженного экспоненциального развития, или по другому – «информационного взрыва». Примерно с 2008 г. объем информации, вновь генерируемой в сети Интернет, стал удваиваться в течение, примерно, полутора-двух лет. При этом примерно треть передаваемых данных составляют автоматически сгенерированные данные, т.е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к глобальной сети, или как его называют – «Интернету вещей» [58].
2. В 2010-х годах появились и стали доступны принципиально новые IT-решения, позволяющие в режиме реального времени обрабатывать практически безразмерные массивы данных самого различного формата. Причем эти решения сразу же стали реализовываться не только как программные платформы, устанавливаемые на серверы, но и как облачные решения, при использовании которых от организации не требовалось наличия дорогостоящей компьютерной инфраструктуры [58].
3. В-третьих, к концу 2000-х годов западные поведенческие и когнитивные науки из фазы фундаментальных исследований перешли в стадию разработок эффективных технологий анализа поведения и социальных связей в обществе [58].

Таким образом, формирование глобального электронного, постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и огромных компаний до небольших групп и отдельных индивидуумов собственно и послужило базисом появления Больших Данных. С тех пор направление Больших Данных стало ведущим в сфере информационных технологий.

Анализ накопленного за последние годы опыта применения технологий Больших Данных позволяет выделить несколько ключевых черт, отличающих их от всех других информационных технологий. К ним относятся [58]:

- во-первых, огромные массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т.п., пополняемые непрерывно в режиме реального времени. Согласно имеющейся статистике, 60% этой информации носит неструктурированный, в основном текстовой характер и 40% – составляет структурированная, или табличная информация. В последние годы в общем объеме Больших Данных постоянно нарастает доля информации структурированного характера, поступающей от устройств, имеющих связь с Интернетом;
- во-вторых, специально спроектированные программные платформы, где Большие Данные любого объема могут храниться в удобном для обработке виде. Особо надо подчеркнуть, что эти архивы отличаются от стандартных баз данных. Отличительной чертой этих хранилищ является то, что структурированная и неструктурированная информация могут обрабатываться совместно, как единое целое;
- в-третьих, наличие различного рода математического, прежде всего, статистического инструментария для обработки Больших Данных и получение результатов в виде, понятном для человека. Причем, при анализе Больших Данных используются не только традиционные методы математической статистики, но и интеллектуальные алгоритмы обработки данных.

В соответствии с данными исследования [58], не более 0,6% информации, находящейся в Интернет, подпадает под категорию Больших Данных, т.е. накапливается, хранится и перерабатывается. В этом же исследовании указывается, что потенциально в качестве Больших Данных может использоваться порядка 23% всей хранимой в настоящее время информации.

Технологии Больших Данных основаны прежде всего на методах статистического и интеллектуального анализа данных, применяемых на огромных, постоянно пополняемых массивах данных. Эти технологии позволяют [58]:

- *проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам.* Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации, с теми или иными его действиями;
- *осуществлять многомерный статистический математический анализ.* Этот анализ позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Корреляции не отвечают на вопрос – почему. Они показывают вероятность, с которой при изменении одного фактора изменяется и другой. В каком-то смысле Большие Данные представляют собой альтернативный традиционной науке метод познания действительности. Теоретические модели отвечает на вопрос – почему, а затем, выявив причинно-следственные закономерности, позволяют

формировать рекомендации о порядке действий. В случае выявления корреляционных закономерностей в Больших Данных, стадия выявления первопричины отсутствует, а сразу выявляется закономерная связь различных факторов. При этом, если факторы тесно взаимосвязаны, то на один из факторов возможно осуществить воздействие для достижения целенаправленного изменения связанного с ним фактора;

- *прогнозировать*. На основе классификаций и аналитических выкладок осуществляется прогнозирование, суть которого состоит в том, чтобы на основе выявленной корреляционной связи факторов определить наиболее целесообразный способ воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п. был преобразован в другой.

Большие Данные как прорывная информационная технология были быстро осознаны такими странами как США, Великобритания и Япония. 29 марта 2012 г. администрация Б. Обамы выступила с инициативой «Big Data Research and Development Initiative». Этой инициативой предусматриваются вложение значительных объемов ресурсов и проведение комплексных мероприятий в целях активного использования технологий Больших Данных в интересах ключевых направлений политики США [58].

Большие Данные, в первую очередь, были использованы в маркетинге, инвестиционном бизнесе, в продажах и т.п. В дальнейшем технологии Больших Данных стали использоваться в таких сферах как разведка и контрразведка, военное дело, геостратегия, а также в информационном противоборстве [58].

Помимо непосредственно разведки и контрразведки, технологии Больших Данных начали использоваться для выявления глубоких паттернов поведения в социальной среде.

В последние годы создана, по сути, новая наука – социодинамика, которая обобщает эмпирические закономерности, полученные в результате применения технологий Больших Данных к огромным массивам информации, содержащейся в архивах крупнейших социальных платформ на основе Web и Web 2.0, таких как Google, Facebook, Twitter и т.п. Эти эмпирические закономерности сегодня используются для отработки практического инструментария внешнего воздействия, управления и манипулирования социальными группами любых масштабов и любого уровня структурированности, а также для сборки и деструкции социальных субъектов. Именно применение Больших Данных к информации, полученной из социальных сетей, позволило осуществить прорыв в отработке инструментария внешнего социального управления поведением [58].

3.10.3 Средства прогнозирования на основе технологий «Больших Данных»

Еще одним направлением эффективного применения технологий Больших Данных является прогноз развития социальных, политических, военных и экономических процессов. При этом к началу нулевых годов

специалисты, ведущие исследования в этой сфере, сформулировали по меньшей мере, три фундаментальных положения [58]:

- используя самые изощренные и эффективные методы, можно прогнозировать процессы, но не события;
- прогнозы с высокой степенью вероятности можно делать в отношении групп различной размерности, но не отдельных индивидуумов;
- знания о действиях групп и индивидуумов в одной ситуации не позволяет давать точные прогнозы о подобных действиях, осуществляемых в другой ситуации.

Соответственно, оказалось, что различного рода прогнозы, базирующиеся на традиционных выборках, построении сценариев, экстраполяции не обладают высоким уровнем адекватности. Развитие Интернета дало возможность оперировать Большими Данными относительно человеческого поведения, намерений, желаний и т.п. Прогнозирование на основе Больших Данных состоит в извлечении нетривиальных выводов из заранее известных характеристик, признаков и сведений об объектах. Использование Больших Данных из Интернета, как огромного, пополняемого в режиме реального времени поведенческого архива для прогнозирования развивается по трем ключевым направлениям [58]:

- прямой интеллектуальный анализ общедоступных данных, предоставляемых поисковыми системами и различного рода социальными сетями и платформами;
- создание рекомендательных систем, которые прогнозируют различного рода выбор субъектов и групп, и на этой основе рекомендуют им что угодно – от книг до кандидатов в президенты;
- создание сложных прогностических систем, использующих разнородные данные, получаемые из открытой и закрытой части глобальной сети, обрабатываемые с помощью большинства известных методов интеллектуального анализа данных.

В качестве одного из наиболее ярких примеров успешного создания средства разведки как сложной прогнозной системы можно привести проект Recorded Future. Система Recorded Future базируется на трех основных элементах [58].

1. *Поисковая система третьего поколения*, которая ищет не только объекты, соответствующие поисковым запросам, и не только связи между документами, но и взаимосвязи между объектами, их характеристиками и отношениями, содержащимися в различных документах [58].

2. *Разделение информационного поля на составляющие – события, мнения, реакции*. В Recorded Future выделено три класса сообщений. Первый – это сообщения о событиях. События – это длящиеся определенный, достаточно небольшой период времени устойчивые конфигурации, которые характеризуются единством времени, места, участников и т.п. К событиям Recorded Future относит то, что может быть интерпретировано как факты, то, что реально произошло или происходит в данный момент. Второй – это мнения. К мнениям относятся любые сообщения относительно прошлых, настоящих

или будущих событий, высказанные в авторитетных источниках, либо авторитетными людьми. Наконец, третий – это реакции. Здесь принимаются во внимание любые спонтанные реакции людей на те или иные ожидаемые события, зафиксированные в различного рода текстовых сообщениях. Такое разделение на три сегмента информационного поля, как выяснилось, позволяет достаточно хорошо улавливать как господствующие тенденции и опережающим образом реагировать на их изменения, так и выявлять слабые сигналы [58].

3. *Рассмотрение Интернета как огромной распределенной сетевой базы неструктурированных данных.* Recorded Future использует поисковик, работающий в сегментированном информационном пространстве в масштабе огромной сетевой базы данных. В сетевой базе данных разные объекты и их характеристики связаны друг с другом прямыми, обратными и опосредованными связями. Соответственно, такой подход позволяет выявлять не только явные и очевидные связи, но и вести так называемый латентный анализ, т.е. получать неочевидные, а иногда даже и абсолютно не предполагаемые связи и отношения. К тому же обрабатывать огромное количество информации в алгоритмическом режиме. Т.е. оперировать информационными массивами, непосильными для непосредственной обработки человеком [58].

В настоящее время Recorded Future используется в трех сферах: государственной разведке и безопасности, в бизнесе, и в финансах для разработки инвестиционных стратегий [58].

Другим ярким примером прогностических систем нового поколения является система Quid. Эта система создана известным американским программистом и разработчиком Ш. Горли на деньги знаменитого П. Тиля, чья разведывательная программа Palantir является давно и эффективно используемым средством американского разведывательного сообщества [58].

Таким образом, Большие Данные обеспечили появление новых, на порядок более эффективных, чем раньше, методов прогнозирования научно-технических, инженерно-технологических, инвестиционных, политических, социальных и военных процессов. Эти методы в совокупности с методиками глубокого анализа на основе все тех же Больших Данных позволяют говорить о создании принципиально нового вида информационного оружия, а именно – прогностических средств. Этот вид оружия может быть использован как обеспечивающий механизм для разработки и применения традиционных вооружений.

3.10.4 Средства манипуляции и формирования поведения социальных групп на основе технологий «Больших Данных»

Как показано выше, наличие огромного всеобъемлющего поведенческого архива позволило компаниям-владельцам Больших Данных использовать их для предсказания поведения. Вместе с тем прогнозирование поведения социальных групп в тех или иных условиях позволяет решить и другую задачу – выбора условий и воздействий, при которых бы целевая социальная группа

действовала бы необходимым, заранее predetermined, образом. В работе [59] для такой манипуляции в отношении целевых социальных групп введено понятие «подталкивание» («nudge»).

«Подталкивание» представляет собой комплекс способов использования поведенческих стереотипов, психофизио-логических реакций и технологий Больших Данных для целенаправленной коррекции поведения тех или иных конкретных социальных групп. При этом выбор тех или иных факторов воздействия, которые обеспечивают реализацию эффекта «подталкивания», осуществляется на основе предсказательной аналитики полученной по итогам обработки Больших Данных [58].

Летом 2013 года было объявлено, что команды по использованию этой технологии создаются в большинстве министерств США, связанных с социальными вопросами. На них возложена задача «подталкивания» американцев к правильным с точки зрения правительства решениям не на основе объяснений, а путем использования поведенческих стереотипов, привычек и психофизиологических реакций. При этом американские СМИ высказали подозрение, что подобные команды создаются и в других, в том числе разведывательных ведомствах. Однако их финансирование реализуется через секретные статьи бюджета, и поэтому их существование не афишируется [58].

Профессионалы «подталкивания», развивая поведенческую политику, исходят из нескольких основных принципов.

- Для решения своих поведенческих проблем люди нуждаются во вмешательстве третьих лиц. Наилучшим кандидатом на эту роль является государство.
- Эксперты, изучая то влияние, которое в реальной жизни оказывают на благосостояние те или иные акты выбора, принимают от имени индивидов решения лучше тех, на которые индивиды способны сами.
- Любые стимулирующие схемы, которые возлагают на людей ответственность за последствия их прошлых действий, неэффективны. Вместо них необходимы схемы, которые немедленно вознаграждают или наказывают людей за будущие последствия их текущих действий – последствия, которые сами они неспособны осознать и учесть.
- С точки зрения политики то, как люди ощущают себя в обществе, важнее того, что они желают, или того, что они делают.

Ключевую роль в технологиях «подталкивания» играют Большие Данные. Именно Большие Данные позволяют, в зависимости от поставленной задачи проводить классификацию групп и ситуаций, осуществлять анализ и прогноз, а главное – искать факторы, обеспечивающие нужное поведение целевых групп в конкретных ситуациях. И, наконец, они в режиме реального времени позволяют отслеживать эффективность «подталкивания» [58].

Стоит отметить, что при наличии соответствующих Больших Данных фактически нет никаких ограничений для использования технологий «подталкивания» не только в отношении граждан собственной страны, но и населения любых государств мира. Таким образом, в настоящее время АНБ и

другие государственные структуры США разрабатывают и переходят к практическому использованию технологий управления групповым и массовым поведением в других странах мира – как в странах-союзниках, так и в странах-противниках.

При наличии соответствующих Больших Данных «подталкивание» может рассматриваться как эффективное информационно-психологическое оружие следующего поколения. Хотя, с учетом принципов и технологий, на которых построена система «подталкивания», более точным является не привычное наименование информационно-психологического оружия, а скорее отнесение этой технологии к поведенческому оружию, базирующемуся на симбиозе высокопроизводительных технических средств обработки, технологиях Больших Данных, достижениях объективной психологии и когнитивных науках [58].

Заключение

В работе предложен понятийный аппарат и представлен авторский подход к классификации информационного оружия в технической сфере. Классифицированы информационно-технические воздействия. Проведен анализ средств, способов и примеров применения для наиболее распространенных информационно-технических воздействий. Обоснованы их определения и их классификация.

Литература

1. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.
2. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.
3. Бедрицкий А. В. Информационная война: концепции и их реализация в США / Под ред. Е.М. Кожокина. – М.: РИСИ, 2008. – 187 с.
4. Новиков В. К. Информационное оружие – оружие современных и будущих войн. – М.: Горячая линия - Телеком, 2011. – 264 с.
5. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия // Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 104-146.
6. Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства. – М.: Горячая линия - Телеком, 2006. – 192 с.
7. Шеховцов Н. П., Кулешов Ю. Е. Информационное оружие: теория и практика применения в информационном противоборстве // Вестник Академии военных наук. 2012. № 1 (38). С. 35-40.
8. Паршакова Е. Д. Информационные войны: учебное пособие – Краматорск: ДГМА, 2012. – 92 с.

9. Информационная война и защита информации. Словарь основных терминов и определений. – М.: Центр стратегических оценок и прогнозов, 2011. – 68 с.
10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
11. Прокофьев В. Ф. Тайное оружие информационной войны. Воздействие на подсознание. – М.: Синтег, 2003. – 430 с.
12. Расторгуев С. П. Информационная война. – М.: Радио и связь, 1999. – 416 с.
13. Буренок В.М., Ивлев А.А., Корчак В.Ю. Развитие военных технологий XXI века: проблемы планирование, реализация. – Тверь: Издательство ООО «КУПОЛ», 2009. – 624 с.
14. Буянов В. П., Ерофеев Е. А., Жогла Н. Л., Зайцев О. А., Курбатов Г. Л., Петренко А. И., Уфимцев Ю. С., Федотов Н. В. Информационная безопасность России – М.: Издательство «Экзамен», 2003. – 560 с.
15. Абдурахманов М. И., Баришполец В. А., Баришполец Д. В., Манилов В. Л. Геополитика, международная и национальная безопасность. Словарь основных понятий и определений / Под общей ред. В.Л. Манилова. – М.: РАЕН, 1998. – 256 с.
16. Хогг О. Эволюция оружия. От каменной дубинки до гаубицы / Пер. с англ. Л.А. Игоревского. – М.: ЗАО Центрполиграф, 2008. – 250 с.
17. Колин К. К. Социальная информатика. – М.: Академический проект, 2003. – 432 с.
18. Остапенко О. Н., Баушев С. В, Морозов И. В. Информационно-космическое обеспечение группировок войск (сил) ВС РФ: учебно-научное издание. – СПб.: Любавич, 2012. – 368 с.
19. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны – реальная угроза национальной безопасности. – М.: КРАСАНД, 2011. – 96 с.
20. Проблемы безопасности программного обеспечения / Под ред. П.Д. Зегжды. – СПб.: ГТУ, 1995. – 200 с.
21. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.
22. Медведовский И. Д., Семьянов П. В., Платонов В. В. Атака через Интернет / Под ред. П.Д. Зегжды. – СПб.: Изд. НПО «Мир и семья-95», 1997. – 277 с.
23. DoS-атака // Wikipedia [Электронный ресурс]. 19.05.2016. – URL: <https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0> (дата доступа 19.05.2016).
24. Марков А. С., Фадин А. А. Организационно-технические проблемы защиты от целевых вредоносных программ // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.
25. Duqu: A Stuxnet-like malware found in the wild, technical report. Laboratory of Cryptography of Systems Security (CrySyS). – Budapest: Budapest University of Technology and Economics Department of Telecommunications, 2011.

- 60 p. – URL: <http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf> (дата доступа 20.08.2016).
26. Вирус Regin // Security Lab [Электронный ресурс]. 28.05.2015. – URL: <http://www.securitylab.ru/analytics/473080.php> (дата доступа 14.08.2016).
27. Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации: учебное пособие. – М.: Издательский центр «Академия», 2006. – 256 с.
28. Шабанов А. Программные закладки в бизнес-приложениях // Anti-Malware [Электронный ресурс]. 13.01.2011. – URL: http://www.anti-malware.ru/software_backdoors# (дата доступа 14.08.2016).
29. Дождиков В. Г., Салтан М. И. Краткий энциклопедический словарь по информационной безопасности. – М.: ИАЦ Энергия, 2010. – 240 с.
30. Зайцев О. Современные клавиатурные шпионы // Компьютер Пресс [Электронный ресурс]. 2006. № 5. – URL: <http://www.compress.ru/Archive/CP/2006/5/23/> (дата доступа 14.08.2016).
31. Виноградов А. А. Функциональность, надежность, киберустойчивость в системах автоматизации критических инфраструктур [Доклад] // Конференция «Региональная информатика-2012». – СПб.: ОАО «НПО «Импульс», 2012.
32. Каталог АНБ США. 2014. 48 с. [Электронный ресурс]. – URL: <http://s3r.ru/13/01/2014/novosti/raskryit-spisok-apparatnyih-zakladok-anb-ssha-dlya-tehniki-cisco-huawei-i-juniper-katalog/attachment/48-stranits-kataloga-abn-ssha/> (дата доступа 14.08.2016).
33. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60-65.
34. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. № 4 (7). С. 60-68.
35. Китайские закладки. Голый король // Security Lab [Электронный ресурс]. 30.09.2012. – URL: http://www.securitylab.ru/contest/430512.php?pagen=7&el_id=430512 (дата доступа 14.08.2016).
36. Марков А. С., Цирлов В. Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.
37. Тихонов А. Ю., Аветисян А. И. Развитие taint-анализа для решения задачи поиска программных закладок // Труды Института системного программирования РАН. 2011. Т. 20. С. 9-24.
38. Гайсарян С. С., Чернов А. В., Белеванцев А. А., Маликов О. Р., Мельник Д. М., Меньшикова А. В. О некоторых задачах анализа и трансформации программ // Труды Института системного программирования РАН. 2004. Т. 5. С. 7-40.
39. Чукляев И. И. Анализ уязвимостей в исходных кодах программного обеспечения статическими и динамическими методами // XII Всероссийское совещание по проблемам управления «ВСПУ-2014», 16-19 июня 2014 г. – М., 2014. – С. 9232-9242.

40. Шурдак М. О., Лубкин И. А. Методика и программное средство защиты кода от несанкционированного анализа // Программные продукты и системы. 2012. № 4. С. 176-180.
41. Язов Ю. К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.
42. Сердечный А. Л. Инновационный подход к защите информации в виртуальных вычислительных сетях, основанный на стратегии обмана // Информация и безопасность. 2013. № 3. С. 399-403.
43. Булойчик В. М., Берикбаев В. М., Герцев А. В., Русак И. Л., Булойчик А. В., Герцев В. А., Зайцев С. И. Разработка и реализация комплекса имитационных моделей боевых действий на мультипроцессорной вычислительной системе // Наука и военная безопасность. 2009. № 4. С. 32-37. – URL: <http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2009/12076-razrabotka-i-realizacija-kompleksa-imitacionnyh> (дата доступа 30.07.2014).
44. Резяпов Н., Чесноков С., Инюхин С. Имитационная система моделирования боевых действий JWARS // Зарубежное военное обозрение. 2008. № 11. С. 27-32. – URL: <http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7599-imitacionnaja-sistema-modelirovanija-boevyh> (дата доступа 17.08.2016).
45. Резяпов Н. Развитие систем компьютерного моделирования в вооруженных силах США // Зарубежное военное обозрение. 2007. № 6. С. 17-23. – URL: <http://pentagonus.ru/publ/11-1-0-222> (дата доступа 18.08.2016).
46. Новиков Д. А. Иерархические модели военных действий // Управление большими системами: сборник трудов. 2012. № 37. С. 25-62.
47. Меньшаков Ю. К. Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.
48. Чуκληев И. И., Морозов А. В., Болотин И. Б. Теоретические основы оптимального построения адаптивных систем комплексной защиты информационных ресурсов распределенных вычислительных систем: монография. – Смоленск: ВА ВПВО ВС РФ, 2011. – 227 с.
49. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с.
50. Емельянов С. Л. Техническая разведка и технические каналы утечки информации // Системи обробки інформації. 2010. № 3 (84). С. 20-23.
51. Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 216-223.
52. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Том 16. № 1. С. 115-118.
53. Пахомова А. С., Пахомов А. П., Юрасов В. Г. Об использовании классификации известных компьютерных атак в интересах разработки

структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 81-86.

54. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description // Cigital Inc. 2008. Vol. 3.

55. Зенин А. Разведка в сухопутных войсках США на основе анализа открытых источников информации // Зарубежное военное обозрение. 2009. № 5 С. 32-38. URL: <http://pentagonus.ru/publ/80-1-0-1183> (дата доступа 17.08.2016).

56. Кондратьев А. Разведка с использованием открытых источников информации в США // Зарубежное военное обозрение. 2010. № 9. С. 28-32. URL: <http://militaryarticle.ru/zarubezhnoe-voennoe-obozenie/2010-zvo/7969-razvedka-s-ispolzovaniem-otkrytyh-istochnikov> (дата доступа 30.08.2016).

57. Разведка средствами Интернет // IT-сектор [Электронный ресурс]. – URL: <http://it-sektor.ru/razvedka-sredstvami-internet.html> (дата доступа 17.08.2016).

58. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.

59. Thaler R. H., Sunstein C. R. Nudge: Improving decisions about health, wealth, and happiness. – Yale: Yale University Press, New Haven, CT, 2008. – 293 p.

60. Кожевников Д. А., Максимов Р. В., Павловский А. В. Способ защиты вычислительной сети (варианты) // Патент на изобретение RU 2325694 С1. Опубл. 27.05.2008, бюл. № 15.

61. Гречишников Е. В., Стародубцев Ю. И., Белов А. С., Стукалов И. В., Васюков Д. Ю., Иванов И. В. Способ (варианты) управления демаскирующими признаками системы связи // Патент на изобретение RU 2450337 С1. Опубликовано 10.05.2012, Бюл. № 13.

62. Иванов В. А., Белов А. С., Гречишников Е. В., Стародубцев Ю. И., Ерышов В. Г., Алашеев В. В., Иванов И. В. Способ контроля демаскирующих признаков системы связи // Патент на изобретение RU 2419153 С2. Опубликовано: 20.05.2011, Бюл. №14.

63. Хорев А. А. Теоретические основы оценки возможностей технических средств разведки: монография. – М.: МО РФ, 2000. – 255 с.

64. Технические средства видовой разведки: учеб. пособие / Под ред. А.А. Хорева. – М.: РВШ, 1997. – 327 с.

References

1. Makarenko S. I., Chucklyaev I. I. The terminological basis of the informational conflict area. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 13-21 (in Russian).

2. Griniaev S. N. *Pole bitvy – kiberprostranstvo. Teoriia, priemy, sredstva, metody i sistemy vedeniia informatsionnoi voyny* [Battlefield – cyberspace. Theory, techniques, tools, methods and systems of information warfare]. Moscow, Kharvest Publ., 2004. 426 p. (in Russian).

3. Bedritskiy A. V. *Informatsionnaia voina: kontseptsii i ikh realizatsiia v SShA* [Information warfare: concepts and their implementation in the United States]. Moscow, The Russian Institute of Strategic Research, 2008. 187 p. (in Russian).
4. Novikov V. K. *Informatsionnoe oruzhie – oruzhie sovremennykh i budushchikh voyn* [Information weapons – modern weapons and future wars]. Moscow, Goriachaia liniia - Telekom, 2011. 264 p. (in Russian).
5. Petrenko S. A. *Metody informatsionno-tekhnicheskogo vozdviistviia na kibersistemy i vozmozhnye sposoby protivodeistviia* [Methods information technology impact on cyber-systems and possible ways to counter]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk*, 2009, vol. 41, pp. 104-146 (in Russian).
6. Vorontsova L. V., Frolov D. B. *Istoriia i sovremennost' informatsionnogo protivoborstva* [History and modernity of information warfare]. Moscow, Goriachaia liniia - Telekom, 2006. 192 p. (in Russian).
7. Shekhovtsov N. P., Kuleshov Iu. E. *Informatsionnoe oruzhie: teoriia i praktika primeneniia v informatsionnom protivoborstve* [Information warfare: theory and practice in information war]. *Vestnik Akademii voennykh nauk*, 2012, vol. 38, no. 1, pp. 35-40 (in Russian).
8. Parshakova E. D. *Informatsionnye voyny: uchebnoe posobie* [The information war]. Kramatorsk, Donbass state engineering Academy, 2012. 92 p. (in Russian).
9. *Informatsionnaia voina i zashchita informatsii. Slovar' osnovnykh terminov i opredelenii* [Information warfare and information security. A Glossary of key terms and definitions]. Moscow, Center for strategic assessments and forecasts, 2011. 68 p. (in Russian).
10. JP 3-13.1. *Electronic Warfare*. US Joint Chiefs of Staff, 2007. 115 p.
11. Prokofev V. F. *Tainoe oruzhie informatsionnoi voyny. Vozdeistvie na podsoznanie* [Secret weapon of the information war. Impact on the subconscious]. Moscow, Sinteg Publ., 2003. 430 p. (in Russian).
12. Rastorguev S. P. *Informatsionnaia voina* [Information war]. Moscow Radio i Sviaz Publ., 1999. 416 p. (in Russian).
13. Burenok V. M., Ivlev A. A., Korchak V. Ju. *Razvitie voennykh tekhnologii XXI veka: problemy planirovaniia, realizatsiia* [The progress of military technology of the XXI century: problems of planning, implementation]. Tver, KUPOL Publ., 2009. 624 p. (in Russian).
14. Buianov V. P., Erofeev E. A., Zhogla N. L., Zaitsev O. A., Kurbatov G. L., Petrenko A. I., Ufimtsev Iu. S., Fedotov N. V. *Informatsionnaia bezopasnost' Rossii* [Russia's information security] Moscow, Ekzamen Publ., 2003. 560 p. (in Russian).
15. Abdurakhmanov M. I., Barishpolets V. A., Barishpolets D. V., Manilov V. L. *Geopolitika, mezhdunarodnaia i natsional'naia bezopasnost'. Slovar' osnovnykh poniatii i opredelenii* [Geopolitics, international and national security. A dictionary of basic concepts and definitions]. Moscow, Russian Academy of natural Sciences, 1998. 256 p. (in Russian).

16. Khogg O. *Evoliutsiia oruzhiia. Ot kamennoi dubinki do gaubitsy* [The evolution of arms. From stone club to howitzers]. Moscow, Tsentrpoligraf Publ., 2008. 250 p. (in Russian).
17. Kolin K. K. *Sotsial'naia informatika* [Social Informatics]. Moscow, Akademicheskii proekt Publ., 2003. 432 p. (in Russian).
18. Ostapenko O. N., Baushev S. V., Morozov I. V. *Informatsionno-kosmicheskoe obespechenie gruppirovok voisk (sil) VS RF: uchebno-nauchnoe izdanie* [Information and space security groups of troops (forces) of the armed forces]. Saint-Peterburg, Liubavich Publ., 2012. 368 p. (in Russian).
19. Parshin S. A., Gorbachev Iu. E., Kozhanov Iu. A. *Kibervoiny – real'naia ugroza natsional'noi bezopasnosti* [Cyberwarfare is a real threat to national security]. Moscow, KRASAND Publ., 2011. 96 p. (in Russian).
20. Zegzhdy P. D. *Problemy bezopasnosti programmnoho obespecheniia* [Security issues software]. Saint-Peterburg, St. Petersburg state Polytechnical University named after Peter the Great, 1995. 200 p. (in Russian).
21. Makarenko S. I. *Information security*. Stavropol, Sholokhov Moscow State University for the Humanities (Stavropol Branch) Publ., 2009, 372 p. (in Russian).
22. Medvedovskii I. D., Semianov P. V., Platonov V. V. *Ataka cherez Internet* [Attack online]. Saint-Petersburg, "Mir i semia-95" Publ., 1997. 277 p. (in Russian).
23. Denial-of-service attack. *Wikipedia*, 19 May 2016. Available at: https://en.wikipedia.org/wiki/Denial-of-service_attack (accessed 19 May 2016).
24. Markov A. S., Fadin A. A. Organizational and technical problems of protection against targeted malware such as Stuxnet. *Voprosy kiberbezopasnosti*, 2013, vol. 1, no. 1, pp. 28-36 (in Russian).
25. Duqu: A Stuxnet-like malware found in the wild, technical report. *Laboratory of Cryptography of Systems Security (CrySyS)*. Budapest, Budapest University of Technology and Economics Department of Telecommunications, 2011. 60 p. Available at: <http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf> (accessed 20 August 2016).
26. Regin Virus. *Security Lab*, 28 May 2015. Available at: <http://www.securitylab.ru/analytics/473080.php> (accessed 14 August 2016) (in Russian).
27. Kuprijanov A. I., Saharov A. V., Shevtsov V. A. *Osnovy zashchity informatsii* [The basics of information security]. Moscow, Publishing center «Akademia», 2006. 256 p. (in Russian).
28. Shabanov A. Programmnye zakladki v biznes-prilozheniiakh [Backdoors in business applications]. *Anti-Malware*, 13 January 2011. Available at: http://www.anti-malware.ru/software_backdoors# (accessed 14 August 2016) (in Russian).
29. Dozhdikov V. G., Saltan M. I. *Kratkii entsiklopedicheskii slovar' po informatsionnoi bezopasnosti* [Short encyclopedic dictionary of information security]. Moscow, Energiia Publ., 2010. 240 p. (in Russian).
30. Zaitsev O. *Sovremennye klaviaturnye shpiony* [Modern keyloggers]. Computer Press, 2006, no. 5. Available at:

<http://www.compress.ru/Archive/CP/2006/5/23/> (accessed 14 August 2016) (in Russian).

31. Vinogradov A. A. Funktsional'nost', nadezhnost', kiber-ustoichivost' v sistemakh avtomatizatsii kriticheskikh infrastruktur [Functionality, reliability, cyber-resilience in the automation systems of critical infrastructures]. *Konferentsiia "Regional'naia informatika-2012"* [Proceedings of Conference "Regional Informatics-2012"]. Saint-Petersburg, "Impul's" Scientific Production Association, 2012.

32. Catalog of the NSA. 2014. 48 p. Available at: <http://s3r.ru/13/01/2014/novosti/raskryit-spisok-apparatnyih-zakladok-anb-ssha-dlya-tehniki-cisco-huawei-i-juniper-katalog/attachment/48-stranits-kataloga-abn-ssha/> (accessed 14 August 2016).

33. Klyanchin A. I. The NSA's spy catalog. Part 1. Infrastructure. *Voprosy kiberbezopasnosti*, 2014, vol. 3, no. 2, pp. 60-65 (in Russian).

34. Klyanchin A. I. The NSA's spy catalog. Part 2. Operator's workplace. *Voprosy kiberbezopasnosti*, 2014, vol. 7, no. 4, pp. 60-68 (in Russian).

35. Kitaiskie zakladki. Golyi korol [Chinese bookmarks. The naked king]. *Security Lab*. 30 September 2012. Available at: http://www.securitylab.ru/contest/430512.php?pagen=7&el_id=430512 (accessed 14 August 2016) (in Russian).

36. Markov A. S., Tsirlov V. L. Experience in identifying vulnerabilities in software. *Voprosy kiberbezopasnosti*, 2013, vol. 1, no. 1, pp. 42-48 (in Russian).

37. Tikhonov A. Iu., Avetisian A. I. Razvitie taint-analiza dlia resheniia zadachi poiska programmnykh zakladok [Development of taint-analysis for solving the problem of finding software bugs]. *Proceedings of the Institute for System Programming of the RAS*, 2011, vol. 20, pp. 9-24 (in Russian).

38. Gaisarian S. S., Chernov A. V., Belevantsev A. A., Malikov O. R., Melnik D. M., Menshikova A. V. O nekotorykh zadachakh analiza i transformatsii program [On some problems of the analysis and transformation of programs]. *Proceedings of the Institute for System Programming of the RAS*, 2004, vol. 5, pp. 7-40 (in Russian).

39. Chukliaev I. I. Analiz uiazvimostei v iskhodnykh kodakh programmnoogo obespecheniia staticheskimi i dinamicheskimi metodami [The analysis of vulnerabilities in source code of the software static and dynamic methods]. *XII Vserossiiskoe soveshchanie po problemam upravleniia "VSPU-2014"* [XII all-Russia meeting on control problems, "VSPU-2014"], Moscow, 2014. pp. 9232-9242 (in Russian).

40. Shurdak M. O., Lubkin I. A. Metodika i programmnoe sredstvo zashchity koda ot nesanksionirovannogo analiza [The methodology and software tool code protection against unauthorized analysis]. *Programmnye produkty i sistemy*, 2012, no. 4, pp. 176-180 (in Russian).

41. Yazov Yu. K., Serdechnyy A. L., Sharov I. A. Methodical approach for estimation of efficiency of honeypot system. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 55-60 (in Russian).

42. Serdechnyy A. L. The innovation approach, based on strategy of deception, to information security of virtual networks. *Informatsiia i bezopasnost*, 2013, no. 3, pp. 399-403 (in Russian).

43. Buloichik V. M., Berikbaev V. M., Gertsev A. V., Rusak I. L., Buloichik A. V., Gertsev V. A., Zaitsev S. I. Razrabotka i realizatsiia kompleksa imitatsionnykh modelei boevykh deistvii na mul'tiprotsessornoi vychislitel'noi sisteme [Development and implementation of a complex simulation models fighting in a multiprocessor computing system]. *Nauka i voennaia bezopasnost*, 2009, no. 4, pp. 32-37. Available at: <http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2009/12076-razrabotka-i-realizaciya-kompleksa-imitacionnykh> (accessed 30 July 2016) (in Russian).

44. Reziapov N., Chesnokov S., Iniukhin S. Imitatsionnaia sistema modelirovaniia boevykh deistvii JWARS [Simulation the simulation system of hostilities JWARS]. *Zarubezhnoe voennoe obozrenie*, 2008, no. 11, pp. 27-32. Available at: <http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7599-imitacionnaja-sistema-modelirovaniia-boevykh> (accessed 17 August 2016) (in Russian).

45. Reziapov N. Razvitie sistem komp'iuternogo modelirovaniia v vooruzhennykh silakh SShA [Development of systems for computer modeling in the U.S. armed forces]. *Zarubezhnoe voennoe obozrenie*, 2007, no. 6, pp. 17-23. Available at: <http://pentagonus.ru/publ/11-1-0-222> (accessed 18 August 2016) (in Russian).

46. Novikov D. A. Hierarchical models of combat. *Upravlenie bol'simi sistemami*, 2012, no. 37, pp. 25-62 (in Russian).

47. Menshakov Iu. K. *Teoreticheskie osnovy tekhnicheskikh razvedok* [The theoretical basis of technical intelligence]. Moscow, Bauman Moscow State Technical University Publ., 2008. 536 p. (in Russian).

48. Chukliaev I. I., Morozov A. V., Bolotin I. B. *Teoreticheskie osnovy optimal'nogo postroeniia adaptivnykh sistem kompleksnoi zashchity informatsionnykh resursov raspredelennykh vychislitel'nykh sistem: monografiia* [Theoretical Foundations of Optimal Construction of Adaptive Systems of Comprehensive Protection of Information Resources Distributed Computing Systems. Monograph] Smolensk, Military Academy of Army Air Defence Publ., 2011. 227 p. (in Russian).

49. Khoroshko V. A., Chekatkov A. A. *Metody i sredstva zashchity informatsii* [Methods and means of information protection]. Kiev, Iunior Publ., 2003. 504 p. (in Russian).

50. Emelianov S. L. Tekhnicheskaiia razvedka i tekhnicheskie kanaly utechki informatsii [Technical intelligence technical channels of information leakage]. *Sistemi obrobki informatsii*, 2010, vol. 84, no. 3, pp. 20-23 (in Russian).

51. Varlamov O. O. O sistemnom podkhode k sozdaniuu modeli komp'iuternykh ugroz i ee roli v obespechenii bezopasnosti informatsii v kliuchevykh sistemakh informatsionnoi infrastruktury [A systematic approach to creating models of computer threats and its role in information security in the key systems of

information infrastructure]. *Izvestiya SFedU. Engineering sciences*, 2006, vol. 62, no. 7, pp. 216-223 (in Russian).

52. Pakhomova A. S., Pakhomov A. P., Razinkin K. A. To the problem of the development of a structural model of computer intelligence. *Informatsiia i bezopasnost*, 2013, vol. 16, no. 1, pp. 115-118 (in Russian).

53. Pakhomova A. S., Pakhomov A. P., Yurasov V. G. To the implementation of the known computer attacks classification to develop a structural model of computer intelligence. *Informatsiia i bezopasnost*, 2013, vol. 16, no. 1, pp. 81-86 (in Russian).

54. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description. *Cigital Inc*, 2008, Vol. 3.

55. Zenin A. Razvedka v sukhoputnykh voiskakh SShA na osnove analiza otkrytykh istochnikov informatsii [Intelligence in the United States army based on the analysis of open source information]. *Zarubezhnoe voennoe obozrenie*, 2009, no. 5, pp. 32-38. Available at: <http://pentagonus.ru/publ/80-1-0-1183> (accessed 17 August 2016) (in Russian).

56. Kondratev A. Razvedka s ispol'zovaniem otkrytykh istochnikov informatsii v SShA [Intelligence using open sources of information in the United States]. *Zarubezhnoe voennoe obozrenie*, 2010, no. 9, pp. 28-32. Available at: <http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/7969-razvedka-s-ispolzovaniem-otkrytykh-istochnikov> (accessed 30 August 2016) (in Russian).

57. Razvedka sredstvami Internet [The exploration of Internet tools]. *IT-sector*, 2016. Available at: <http://it-sektor.ru/razvedka-sredstvami-internet.html> (accessed 17 August 2016) (in Russian).

58. Larina E. S., Ovchinskii V. S. *Kibervoiny XXI veka. O chem umolchal Edvard Snouden* [Cyberwar XXI century. What silent Edward Snowden]. Moscow, Knizhnyi Mir Publ., 2014. 352 p. (in Russian).

59. Thaler R. H., Sunstein C. R. *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press, New Haven, CT, 2008. 293 p.

60. Kozhevnikov D. A., Maksimov R. V., Pavlovskii A. V. Sposob zashchity vychislitel'noi seti (varianty) [Method of protecting computer network (variants)]. Patent Russia, no. RU 2325694 C1. Publish. 27.05.2008, bul. no. 15 (in Russian).

61. Grechishnikov E. V., Starodubtsev Iu. I., Belov A. S., Stukalov I. V., Vasiukov D. Iu., Ivanov I. V. Sposob (varianty) upravleniia demaskiruiushchimi priznakami sistemy sviazi [Method (variants) control telltale signs of a communication system]. Patent Russia, no. RU 2450337 C1. Publish. 10.05.2012, bul. no. 13 (in Russian).

62. Ivanov V. A., Belov A. S., Grechishnikov E. V., Starodubtsev Iu. I., Eryshov V. G., Alashev V. V., Ivanov I. V. Sposob kontrolya demaskiruiushchikh priznakov sistemy sviazi [Method of control of the telltale signs of a communication system]. Patent Russia, no. RU 2419153 C2. Publish. 20.05.2011, bul. no. 14 (in Russian).

63. Khorev A. A. *Teoreticheskie osnovy otsenki vozmozhnostei tekhnicheskikh sredstv razvedki: monografiia* [The theoretical basis for the estimation of

opportunities of technical means of intelligence. Monograph]. Moscow, The Ministry of Defence, 2000. 255 p. (in Russian).

64. Khorev A. A. *Tekhnicheskie sredstva vidovoi razvedki* [Technical means imagery intelligence]. Moscow, Strategic Rocket Forces Publ., 1997. 327 p. (in Russian).

Статья поступила 26 сентября 2016 г.

Информация об авторе

Макаренко Сергей Иванович – кандидат технических наук, доцент. Доцент кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: устойчивость сетей и систем связи к преднамеренным дестабилизирующим воздействиям; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: Россия, 197198, г. Санкт-Петербург, ул. Ждановская д. 13.

Information Weapon in Technical Area – Terminology, Classification and Examples

S. I. Makarenko

Relevance. For review of information warfare is necessary forming the terminological basis. An information weapon is main term of the terminological basis of information warfare. Theory of information weapon in psychological warfare is widely researched at well-known papers. However, theory of information weapon in technical area has not widely researched. Therefore, forming terminological basis for the information weapon in technical area and its classification is topical. **The aim of this paper** is forming the terminological basis and the classification systems for the information weapon in technical area. **Novelty.** The element of novelty of this paper is forming the new terms and the new classification systems for the review of information weapon in technical area by author's way. Also novelty items are trends of improvement of some types of information weapon which detect by author. **Practical relevance.** The review presented can be used by technical specialists to make a new technology in the areas of the information warfare and the information security. Also this review can be used military specialists for elaborating new forms and methods of armed struggle with use of an information weapon.

Key words: information struggle, information weapon, information warfare, information attack, network attack, virus, software beetle, hardware beetle, neutralizer for tests software, mock object of information area, software for modeling of combat acts, radio reconnaissance, open source Intelligence, Big Date.

Information about Author

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. A. F. Mozhaisky Military Space Academy. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197198, Saint-Petersburg, Zhdanovskaya ulica, 13.