ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 002.001.8

ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ ВОЗДЕЙСТВИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

© 2018 А. С. Дубровин, Т. В. Мещерякова, В. И. Арутюнова

Воронежский институт ФСИН России (г. Воронеж, Россия)
Воронежский институт МВД России (г. Воронеж, Россия)

Приводится уточнение терминологического базиса в области определений и классификации информационно-технического оружия и информационно-технических воздействий применительно к автоматизированным системам специального назначения. Представленный анализ основан на методах системного анализа и логического обобщения известных работ.

Ключевые слова: автоматизированные системы специального назначения, информационно-техническое оружие, информационно-техническое воздействие.

В соответствии со сложившейся в проблематике противоборства в информационной сфере терминологией [3] определим понятие информационно-техническое воздействия (ИТВ) на АССН как основной поражающий фактор информационно-технического оружия, представляющий собой воздействие либо на информационный ресурс АССН, либо на саму АССН или на средства получения, передачи, обработки, хранения и воспроизведения информации в ее составе, с целью вызвать заданные структурные и/или функциональные изменения.

Из данного определения следует основополагающая роль информационно-технического оружия, под которым применительно к рассматриваемой в исследовании проблематике понимается [3] 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 АССН, дезорганизовывать работу технических средств ведомственной инфокоммуникационной инфраструктуры обеспечения функционирования системы управления ОВД, применяемая нарушителем безопасности информации для достижения поставленных целей.

Таким образом очевидно, что информационно-техническое оружие включает технические и программные средства, обеспечивающие несанкционированный доступ к базам данных и нарушение штатного режима функционирования аппаратно-программных средств, классификация видов информационно-технического оружия приводится на рисунке 1.

Исходя из общего определения [1] объектов ИТВ для информационно-технических воздействий в АССН таковыми объектами являются – информация, ее состояния защищенности, средства вычислительной техники, телекоммуникационное оборудование, а также инфраструктура АССН.

Для АССН характерны одиночные и групповые виды ИТВ. При этом по характеру поражающих свойств [1, 4] эти воздействия делятся на высокоточные воздействия (воздействия на определенный ресурс) и комплексные воздействия (воздействия на всю инфраструктуру АССН).

Дубровин Анатолий Станиславович – Воронежский институт ФСИН России, профессор кафедры информационной безопасности телекоммуникационных систем, д. т. н, доцент, asd_kiziltash@mail.ru.

Мещерякова Татьяна Вячеславовна – Воронежский институт МВД России, начальник кафедры автоматизированных информационных систем ОВД, к. ф.-м. н., mescher73@mail.ru.

Арутюнова Валентина Игоревна – Воронежский институт МВД России, адъюнкт кафедры автоматизированных информационных систем ОВД, valentina11011008@yandex.ru.

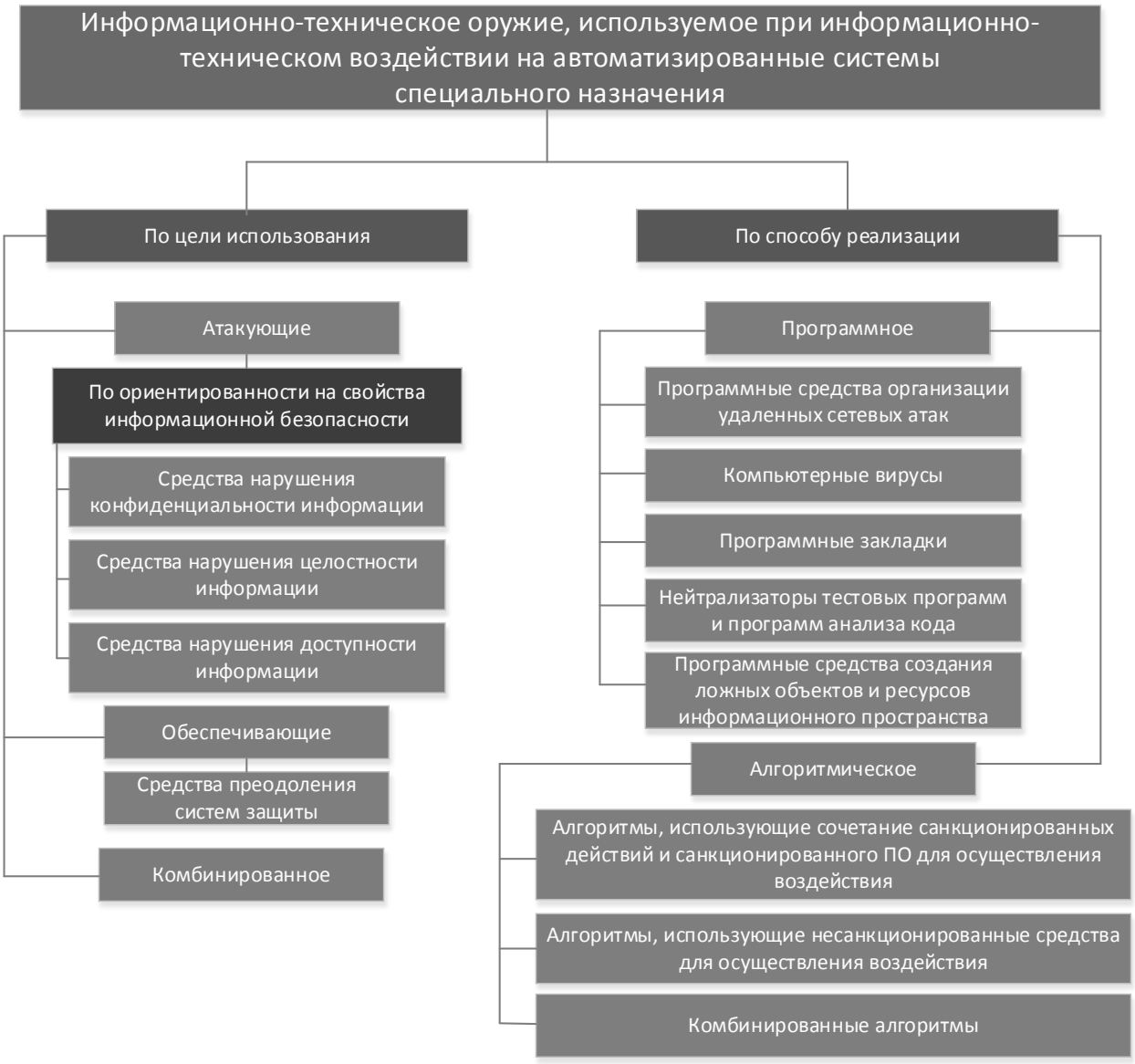

Рисунок 1. Классификация видов информационно-технического оружия, используемого при ИТВ на АССН.

По типу воздействий на информацию или информационный ресурс АССН ИТВ классифицируются на пассивные (перехват, несанкционированный доступ (НСД)) и активные (разрушающие, манипулирующие, блокирующие и отвлекающие воздействия).

По цели использования ИТВ в АССН могут быть классифицированы только как атакующие.

По способу реализации ИТВ, исследуемые в данной работе, могут быть разделены на алгоритмические и программные.

Классификация ИТВ в АССН приводится на рисунке 2.

В качестве информационно-технического оружия для ИТВ в АССН наибольшее распространение получили средства специального программно-математического воздействия. Согласно приведенной в [3] классификации к таким средствам относят отдельные программы или их комплексы, способные выполнить любое подмножество перечисленных ниже функций:

- скрывать признаки своего присутствия в программно-аппаратной среде АССН;
- обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- искажать код программ в памяти АССН;
- сохранять фрагменты информации из памяти АССН 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 телекоммуникационной сети АССН, фальсифицировать информацию, передаваемую по каналам управления;

- противодействовать работе тестовых программ и механизмов защиты информации.

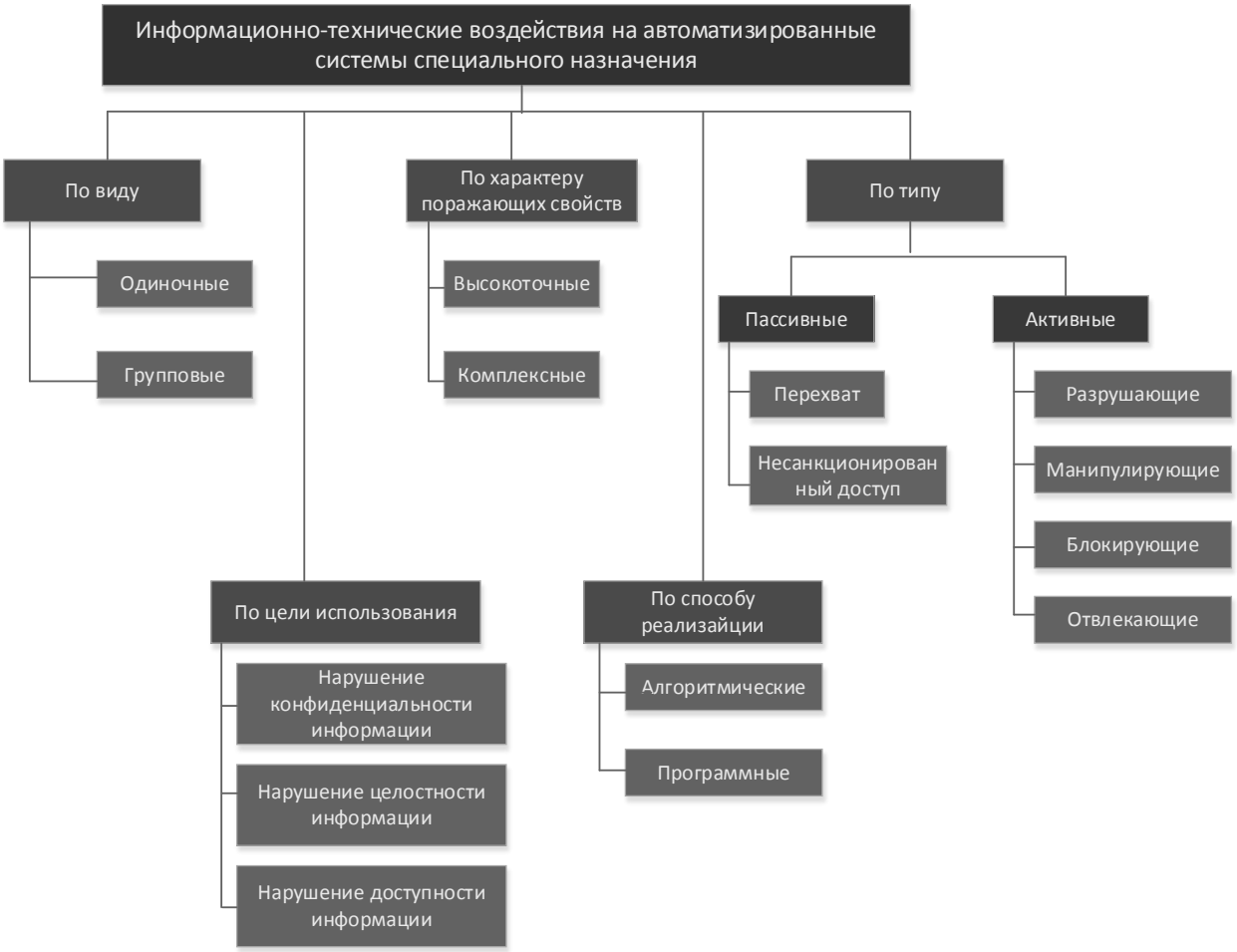

Рисунок 2. Классификация ИТВ на АССН.

Наиболее распространенными на сегодняшний день средствами специального программно-математического воздействия являются эксплойты, компьютерные вирусы, программные закладки, нейтрализаторы тестовых программ и программ анализа кода, программные средства компьютерной разведки в телекоммуникационной части информационного пространства, программные средства ведения разведки на основе открытых источников в семантической части информационного пространства [2].

Схема классификации средств ИТВ представлена на рисунке 3.

Рассмотрим более подробно наиболее распространенные средства ИТВ из представленных на рисунке 3.

Анализатор трафика (сниффер) представляет собой программу, предназначенную для перехвата и последующего анализа, либо только анализа сетевого трафика. Сниффер может анализировать только то, что проходит через сетевую карту автоматизированного рабочего места (АРМ) должностного лица (ДЛ) АССН. Учитывая сетевой характер построение АССН и как следствие - ее сегментирование и маршрутизацию потоков информации, возможны ситуации рассылки внутри одного сегмента АССН пакетов всем АРМ ДЛ. Подобные ситуации дают возможность перехвата данных с любого АРМ ДЛ.

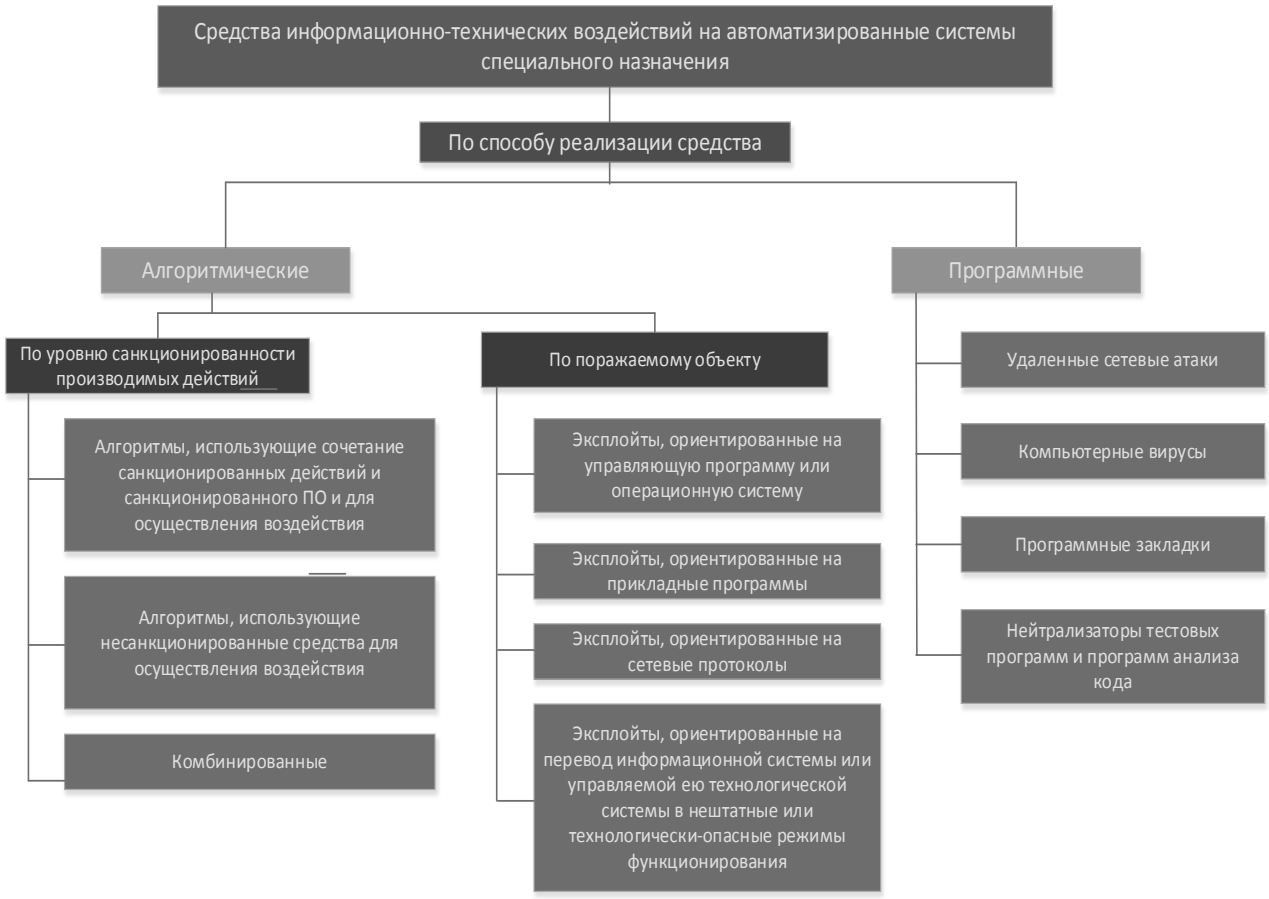

Рисунок 3. Классификация средств ИТВ на АССН.

Программные кейлоггеры (клавиатурные шпионы) принадлежат к группе программ, позволяющих контролировать деятельность должностного лица в процессе его работы на АРМ. Кейлоггеры обеспечивают скрытый мониторинг нажатий клавиш и ведения журнала этих нажатий. Вирусная атака, в основу которой положены идеи кейлоггера, состоит во внедрении между любыми двумя звеньями в цепи прохождения сигнала от нажатия пользователем клавиш на клавиатуре до появления символов на экране с целью видеонаблюдения, перехвата запросов ввода-вывода, подмены системного драйвера клавиатуры, драйвер-фильтра в клавиатурном стеке, перехвата функций ядра путем подмены адресов в системных таблицах, перехвата функций DLL в пользовательском режиме и опроса клавиатуры стандартным задокументированным способом.

Основными представителями класса программных кейлоггеров являютя такие группы вирусных программ как key-loggers, keyloggers, keystroke loggers, key recorders, key trappers, key capture programs. и множество других вариантов названия)

Наиболее характерным вариантом вирусных атак в системах рассматриваемого класса являются так называемые DoS и DDoS-атаки (от англ. Denial of Service и Distributed Denial of Service – соответственно, атака типа «отказ в обслуживании» и распределённая атака этого же типа). Целью такой атаки является доведение атакуемой системы до отказа, то есть создание таких условий, при которых должностные лица АССН не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. В настоящее время DoS и DDoS-атаки являются наиболее распространенными типами вирусных атак, так как позволяют довести до отказа практически любую систему, не оставляя, при этом, юридически значимых улик.

Существующая классификация DoS и DDoS-атак делит их на три категории.

Первая категория DoS и DDoS-атак направлена на насыщение полосы пропускания механизма обработки информации. Результативность такой атаки измеряется в битах в секунду. К данной категории относятся различные виды флудов: UDP, ICMP и прочие потоки сфальсифицированных пакетов.

Вторая категория DoS и DDoS-атак направлена на использование уязвимостей различных протоколов. Такие атаки отвлекают ресурсы сервера либо промежуточного оборудования паразитными пакетами, в результате чего механизм обработки информации оказывается неработоспособным.

Третья категория DoS и DDoS-атак направлена на использование уязвимостей в приложениях и операционных системах (ОС). Данная категория атак приводит к неработоспособности какого-либо приложения или ОС в целом, что создает весьма серьёзные проблемы реализации механизмов антивирусной защиты.

Одним из превалирующих типов сетевых атак, используемых как против отдельных пользователей, так и против отдельных сегментов сети, является MITM-атака (от англ. Man-in-the-Middle – атака типа «человек посредине»). MITM-атака — термин в криптографии, обозначающий ситуацию, когда злоумышленник способен читать и видоизменять по своей воле сообщения, которыми обмениваются абоненты сети, причём ни один из последних не может догадаться о присутствии злоумышленника в канале обмена данными.

Одна из самых старых версий MITM атак является атака типа ARP Poison Routing (от англ. – «отравление» маршрутизатора путем использования протокола определения адреса). В результате атаки злоумышленник, находящийся в одной подсети с атакуемым АРМ ДЛ, имеет возможность перехватывать весь сетевой трафик между объектами атаки. Этот тип атаки считается самым простым для выполнения, но при этом он является наиболее эффективным способом, используемым злоумышленниками.

Подделка DNS (от англ. Domain Naming System – протокол системы доменных имен) представляет собой MITM атаку, целью которой является предоставление ложной DNS информации на АРМ ДЛ, чтобы при попытке просмотра объекта, имеющего заданный IP адрес, этот АРМ ДЛ был направлен на поддельный объект, расположенный по IP адресу, созданным злоумышленником для несанкционированного копирования информации учетной записи с атакуемого АРМ ДЛ.

Атаки с использованием уязвимостей HTTP представляют собой атаки с перехватом сеанса. Когда речь идет о сеансе, имеется в виду некоторое соединение между устройствами, происходящее в данный момент. То есть, происходит взаимодействие, в рамках которого формально соединение устанавливается, поддерживается, причем для завершения соединения требуется определенный процесс. Для обеспечения безопасности сетевых подключений используется механизм шифрования, предоставляемый сервисами протоколов Secure Socket Layers (SSL) или Transport Layer Security (TLS).

Принцип, лежащий в основе атак по перехвату сеанса, основан на возможности перехвата определенных порций данных при его установлении. В последствии эти данные могут использоваться в целях выдачи злоумышленника за одну из взаимодействующих сторон, чтобы получить доступ к информации.

Наиболее распространённым инструментом реализации атак с использованием уязвимостей HTTP является программа Wireshark, предназначенная для анализа пакетов, проходящих в сети. Последующие использование возможностей другой программы - EtherPeek позволяет осуществлять захват проходящих по сети пакетов, их декодирование и предоставление злоумышленнику как самих пакетов, так и содержащейся в них информации в требуемом виде.

Эксплоит – программы, в которых содержатся данные или исполняемый код и которые используют одну или несколько уязвимостей в программном обеспечении на локальном или удаленном АРМ ДЛ с заведомо вредоносной целью.

Существующая классификация эксплоитов предполагает их следующие деление:

- по характеру уязвимости – переполнение буфера, SQL-инъекция, межсайтовый скриптинг (XSS);

- по результату атаки – неавторизованный доступ к данным, выполнение произвольного кода, блокирование доступа.

Основной функцией пакеров является модификация исполняемых файлов, не меняющая функционал последних. При запуске пакованного файла загрузчик производит распаковку и передает управление оригиналу.

По отношению к исполняемым файлам, содержащим вредоносный код пакеры делятся на:

- упаковщики, осуществляющие сжатие файлов;

- крипторы, осуществляющие их шифрование и защиту;

- протекторы, осуществляющие сжатие, шифрование и защиту файлов;

- малварные пакеры, осуществляющие сжатие, шифрование файлов, а так же реали-

зующие функции противодействия антивирусам.

Реализация любого из приведенных типов ИТВ в АССН ОВД приводит к потенциальной возможности срыва выполнения подразделениями полиции своих служебных задач. Ущерб наносимый такого рода действиями может быть существенным.

Рассмотренные ИТВ создают предпосылки для реализации угроз несанкционированного копирования, модификации и блокирования информации в АССН, что приводит к необходимости анализа проблем, связанных с обеспечением защиты информации в этих системах от такого рода угроз информационной безопасности.

ЛИТЕРАТУРА

1. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – М.: Харвест, 2004. – 426 с.

2. Киселев В. В. Классификационная характеристика угроз воздействия вредоносных программ на информационные процессы в компьютерных системах / В. В. Киселев, Д. А. Голубков, В. И. Арутюнова // Вестник Воронежского института ФСИН России. – 2016. – № 2. – С. 49-56.

3. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры / С. И. Макаренко // Системы управления, связи и безопасности. – 2016. – № 3. С. 292-376

4. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.

INFORMATION AND TECHNICAL EFFECTS IN THE AUTOMATED SYSTEMS OF SPECIAL PURPOSE

© 2018 A. S. Dubrovin, T. V. Meshcheryakova, V. I. Arutyunova

The article provides clarification of the terminological basis in the field of definitions and classification of information technology weapons and information technology impacts in relation to automated systems for special purposes. The presented analysis is based on the methods of system analysis and logical generalization of known works.

Key words: automated systems for special purposes, information technology weapons, information technology impact.