Таким образом, как показали результаты анализа рассмотренных типологических видов БТСКД, все фактические размеры ПУ терминалов соответствуют требованиям, что нельзя сказать о размерах сложных знаков на ПУ терминалов и размерах дисплеев.

Список литературы

1. Алефиренко, В. М. Инженерно-психологический анализ панелей управления РЭС: метод. пособие по дисц. «Инженерная психология» для студ. спец. «Моделирование и компьютерное проектирование РЭС», «Техническое обеспечение безопасности» заоч. формы обуч. / В. М. Алефиренко, С. М. Боровиков. – Минск: БГУИР, 2007. – 32 с.

2. Основы инженерной психологии: учебник для техн. вузов / под ред. Б.Ф. Ломова. – М. : Высш. шк., 1986. – 448 с.

3. Рыжковская, М.С. Выбор типологических видов биометрических терминалов для анализа инженерно-психологических, эргономических и эстетических характеристик / М.С. Рыжковская, В.М. Алефиренко // Журнал «Science Time»: Материалы Междунар. науч.-практ. конференций Общества Науки и Творчества за май 2018 года. – Казань, 2018. – № 53. – С. 81–85.

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ ОБЪЕКТОВ РАЗЛИЧНОГО НАЗНАЧЕНИЯ

Алефиренко В.М.,
Белорусский Государственный Университет Информатики и Радиоэлектроники, к.т.н., доцент
Чопик К.В.
Белорусский Государственный Университет Информатики и Радиоэлектроники, магистрант

THE SECURITY THREATS OF INFORMATION INFRASTRUCTURE OF DIFFERENT ASSIGNMENT OBJECTS

Alefirenko V.M.,
Belarus State University of Informatics and Radioelectronics, Ph. D, associated professor
Chopik K.V.
Belarus State University of Informatics and Radioelectronics, master student

Аннотация

В статье рассмотрены типы компьютерных сетей, используемых на объектах различного назначения для передачи данных, возможные виды сетевых атак, осуществляемых злоумышленниками на эти сети, возможные угрозы и источники угроз, а также уязвимости информационных систем.

Abstract

The article describes the types of computer networks used at the different assignment objects for data transmission, possible types of network attacks carried out by attackers on the networks, possible threats and threat sources, as well as vulnerabilities of information systems.

Ключевые слова: информационная инфраструктура, безопасность, информационные системы, компьютерные сети, сетевые атаки, угрозы, источники угроз, уязвимости.

Keywords: information infrastructure, security, information systems, computer networks, network attacks, threats, threat sources, vulnerabilities.

Сети передачи данных и информационные системы в сегодняшнем мире представляют собой одну из важнейших и необходимых подсистем информационной инфраструктуры объектов различного назначения, начиная от обычных офисов различных фирм, объектов торговли, социального назначения (детские сады, учебные заведения, больницы и поликлиники) и заканчивая объектами обеспечения жизнедеятельности людей и существования государства (вокзалы, аэропорты, финансовые и государственные учреждения, промышленные производства, атомные электростанции и т.п.). Все компьютерные сети без исключения имеют одно назначение – обеспечение совместного доступа к общим ресурсам. Однако такой доступ должен быть обеспечен только авторизованным пользователям. Современные информационные технологии позволяют осуществлять авторизованный доступ практически с любой точки земного шара, где для этого имеются соответствующие технические условия. Все это делает привлекательным возможность осуществить доступ несанкционированным пользователям сети, начиная от обычных хакеров с целью получения прибыли (снятие денег со счетов) и кончая профессионалами спецслужб для нанесения ущерба объекту (нарушение функционирования вплоть до вывода его из строя). Очевидно, что при выборе, построении и эксплуатации компьютерной сети конкретного объекта необходимо знать и учитывать особенности сети, ее слабые места (уязвимости), источники угроз и виды

угроз – наиболее вероятные виды атак, которые могут осуществить злоумышленники на конкретную сеть.

Современные сети можно классифицировать по следующим признакам: по типу передачи данных; по области обслуживания; по способу хранения данных; по способу управления ресурсами; по типу среды передачи данных.

Компьютерные сети по типу передачи данных включают в себя два типа технологии передачи: широковещательные сети и сети с передачей от узла к узлу.

Широковещательные сети обладают единым каналом связи, совместно используемым всеми компьютерами сети. Такие сети позволяют адресовать пакет одновременно всем компьютерам с помощью специального кода в поле адреса. Когда передается пакет с таким кодом, его получают и обрабатывают все компьютеры сети. Такая операция называется широковещательной передачей.

Сети с передачей данных от узла к узлу состоят из большого количества соединенных пар компьютеров. Для того, чтобы пакету добраться до пункта назначения, необходимо пройти через ряд промежуточных компьютеров [16].

Компьютерные сети по области обслуживания разделяются на шесть типов: BAN (нательная компьютерная сеть); PAN (персональная компьютерная сеть); LAN (локальная компьютерная сеть); CAN (кампусная компьютерная сеть); MAN (городская компьютерная сеть); WAN (глобальная компьютерная сеть).

Сеть BAN (Body Area Network) представляет собой набор взаимодействующих устройств, которые могут быть встроены/имплантированы в тело человека или закреплены на поверхности тела. Эти устройства отличаются небольшими размерами и небольшой потребляемой мощностью. Радиус действия сети BAN ограничивается 1-2 метрами. Устройства класса BAN могут получить широкое распространение в медицине. Например, небольшие датчики имплантируются в человеческое тело и передают информацию на смартфон или другое устройство, имеющее достаточный объем памяти и возможность выхода в сеть Интернет. Таким образом есть возможность отслеживать состояние конкретного пациента в динамике и получать всегда актуальную информацию о его здоровье [13].

Сеть PAN (Personal Area Network) – персональная компьютерная сеть, обладающая несколько большим масштабом, нежели BAN сеть. Сеть класса PAN предназначена для взаимодействия различных устройств, принадлежащих одному владельцу. Типичным примером такого взаимодействия является взаимодействие между ПК и беспроводной мышкой или клавиатурой. Кроме беспроводных технологий в основе сети PAN лежат также технологии USB или FireWire. Радиус действия PAN сети может быть ограничен несколькими сантиметрами, а может достигать примерно 30 метров [13].

Сеть LAN (Local Area Network) – это компьютерная сеть, которая, покрывает небольшую территорию, располагаясь в одном или нескольких зданиях. В LAN широко используются проводные соединения, большинство из которых выполняется с помощью медных проводов, а некоторые – оптоволоконных. Обычно, проводные сети работают на скоростях от 100 Мбит/с до 1 Гбит/с. Более современные LAN могут работать со скоростью 10 Гбит/с. Наиболее распространенным стандартом проводного соединения является стандарт IEEE 802.3, обычно называемый Ethernet [15].

Сеть CAN (Campus Area Network) объединяет несколько локальных сетей в одну. Например, у нас есть институт, у которого есть общежития и есть корпуса. Каждое отдельное общежитие или корпус – это локальная сеть, в которой устройства физически, чаще всего, соединены витой парой, а каждый корпус соединяется уже оптической линией связи [13].

Сеть MAN (Metropolitan Area Network) – это сеть в масштабах города. К MAN сети относят городские телевизионные и телефонные сети. Радиус таких сетей достигает 10-15 километров. Такие сети обычно строятся и управляются специальными компаниями (провайдерами), которые предоставляют пользователям доступ в Интернет [13].

Сеть WAN (Wide Area Network) соединяет локальные сети, которые могут располагаться в географически удаленных областях. Глобальная сеть похожа на большую локальную компьютерную сеть, но существуют важные различия: управление локальными сетями осуществляется различными организациями; могут соединяться сети, использующие различные виды сетевых технологий; с помощью каналов связи могут связываться отдельные компьютеры с локальными сетями [15].

По способу хранения данных различают три основных технологии обеспечения доступа к данным систем хранения: SAS (Server Attached Storage); NAS (Network Attached Storage); SAN (Storage Area Network).

Технология SAS – традиционная система хранения данных, присоединенная к серверу. Основное преимущество – низкая цена и простота организации.

Технология NAS отличается улучшенной архитектурой файл-сервера и является идеальным вариантом для организации работы серверов с минимальными функциями. К преимуществам относят независимость от операционной системы компьютеров и сервера. К недостаткам – конфликты с трафиком локальной и беспроводной сети.

Технология SAN – это система, которая позволяет организовать распределенный доступ к устройствам хранения данных между серверами и компьютерами, независимая от локальной и беспроводной сети. К преимуществам такой сети относят: независимость от технологии, от систем хранения данных и серверов; централизованное управление сетью; высокое быстродействие [14].

По способу управления ресурсами сети делятся на два типа: с выделенным сервером и одноранговые.

В сетях с выделенным сервером, основные функции выполняет сервер, обеспечивая доступ пользователей к имеющимся ресурсам. Если сервер (или несколько серверов одновременно) – это мощный компьютер, на который ложится основная нагрузка, то остальные компьютеры – это рабочие станции.

В одноранговых сетях все компьютеры обладают равными правами, и управление может осуществляться с любого из них [17].

По типу среды передачи данных компьютерные сети разделяются на две группы: проводные и беспроводные.

Проводные сети – это сети, каналы связи которых построены с использованием медных или оптических кабелей.

Беспроводные сети – это сети, в которых для связи используются беспроводные каналы связи, например, радио, СВЧ, инфракрасные или лазерные каналы [7].

Классификация компьютерных сетей, проведённая по рассмотренным выше признакам, представлена на рисунке 1.

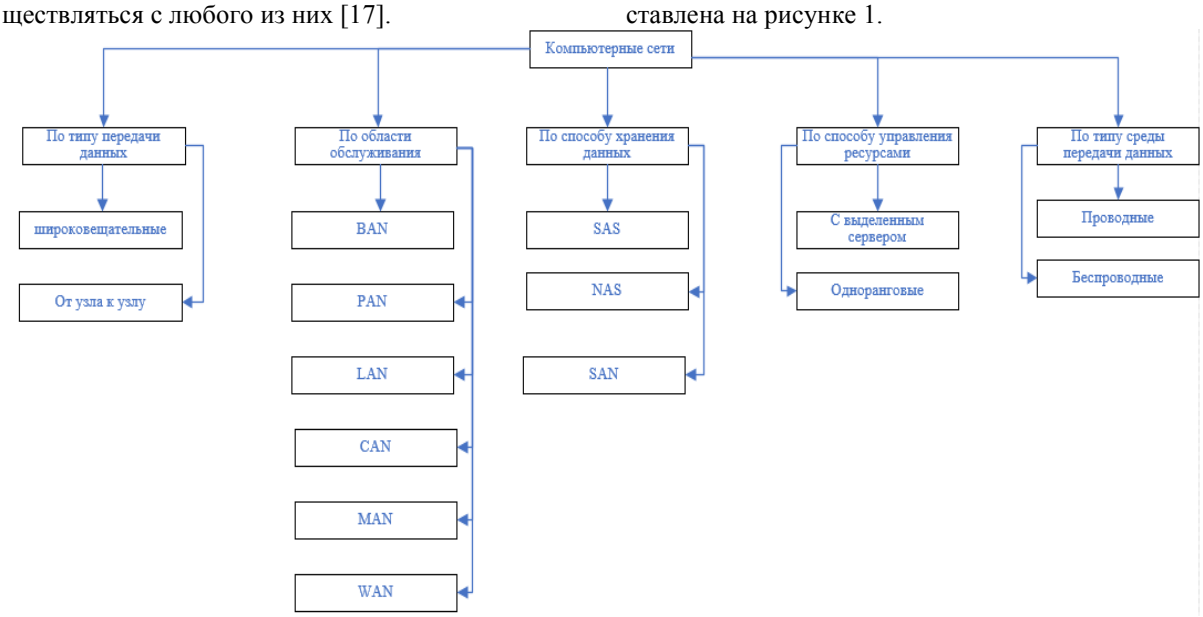

Рисунок 1 – Классификация типов компьютерных сетей

Все типы рассмотренных компьютерных сетей, находящиеся на тех или иных объектах, могут быть подвергнуты сетевым атакам со стороны с целью получения необходимой информации или нарушения функционирования объекта.

Сетевые атаки делятся на две большие группы:

- пассивные;
- активные.

Активной называется такая атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения [8].

Активные атаки, в свою очередь, разделяются на следующие типы:

- атака Man In The Middle;
- DoS-атака;
- Reply-атака.

Атака Man In The Middle – это такой вид сетевой атаки, при которой злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом [7].

Одним из примеров атаки Man In The Middle является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передаёт сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником.

Существует несколько способов проведения атаки Man In The Middle. К ним относятся:

- создание двойника выходной точки, то есть при создании точной копии точки доступа, злоумышленник может получить доступ к каналу передачи данных;
- ARP-spoofing – атака основана на том, что протокол ARP не проверяет подлинности ARP-запросов и ARP-ответов, таким образом сетевое оборудование будет обрабатывать ARP-ответ без запроса [2];
- подмена DHCP-сервера основана на том, что у клиента нет возможности аутентифицировать DHCP-сервер.

DoS-атака существенно отличается от других видов атак. В данном случае цель злоумышленника не состоит в получении доступа к сети, а состоит в том, чтобы сеть стала недоступной для обычного использования за счет превышения допустимых пределов функционирования сети [9]. Реализация DoS-атак может быть проведена следующими способами:

- HTTP-флуд – представляет собой генерирование большого количества HTTP-запросов к серверу жертвы;
- SYN-флуд – принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы,

переполняет на сервере жертвы очередь на подключения;

- UDP-флуд – принцип атаки заключается в отправке множества UDP-пакетов на определённые или случайные номера портов удалённого сервера жертвы, который для каждого полученного пакета должен определить соответствующее приложение;

- ICMP-флуд – принцип атаки заключается в том, что компьютер-жертва получает особым образом подделанный эхо-запрос, после которого он перестает отвечать на запросы вовсе;

- MAC-флуд – принцип атаки заключается в отправке множества пустых Ethernet-фреймов с различными MAC-адресами, которыми заполняется память коммутатора.

Replay-атака – это пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа. На самом деле Replay-атака является одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип атаки [8].

Пассивной называется такая атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика [8].

Пассивные атаки могут быть следующие:

- Snooping (подслушивание);
- парольная атака;
- скомпрометированный ключ атаки.

Snooping означает подслушивание, то есть злоумышленник будет слышать разговор который происходит между двумя компьютерами в сети. Это может произойти в закрытой системе, а также через Интернет. При подслушивании конфиденциальные данные, передаваемые по сети, могут быть доступны для других пользователей.

При совершении парольных атак злоумышленник получает доступ к компьютеру и ресурсам сети путем получения пароля управления системой. Часто можно увидеть, что злоумышленник изменил сервер и конфигурацию сети и в некоторых случаях даже может удалить данные. Кроме того, данные могут передаваться в разные сети.

Для хранения конфиденциальных данных, может быть использован секретный ключ. Когда ключ находится в распоряжении злоумышленника, такой ключ становится скомпрометированным. Злоумышленник теперь будут иметь доступ к конфиденциальным данным и может внести изменения в данные. Однако, существует также вероятность того, что злоумышленник будет пробовать различные перестановки и комбинации ключа для доступа к другим наборам конфиденциальных данных [4].

Проведенная классификация сетевых атак представлена на рисунке 2.

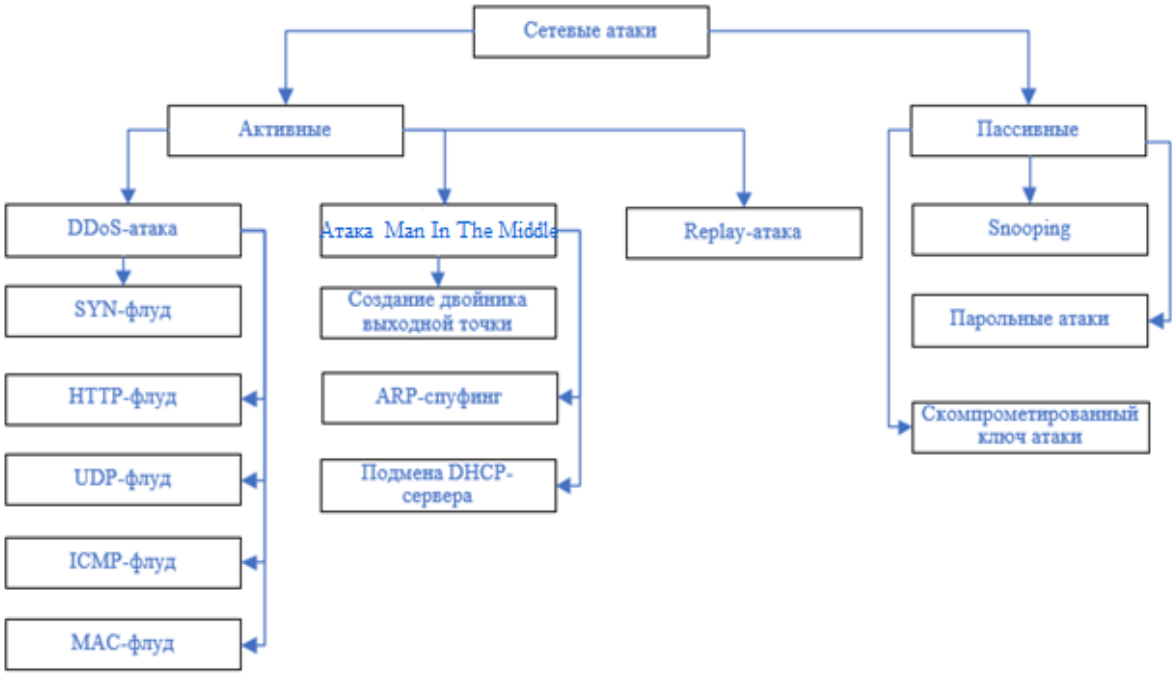

Рисунок 2 – Классификация сетевых атак

Каждая компьютерная сеть может подвергаться различным видам угроз. Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления, например, конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба [19]. Для минимизации ущерба, который может быть нанесён информационной системе, необходимо знать какие источники угроз могут быть использованы против неё. Все источники угроз информационной безопасности можно разделить на три основные группы:

- антропогенные источники угроз;
- техногенные источники угроз;
- стихийные источники угроз.

Антропогенные источники угроз – это субъекты, действия которых могут привести к нарушению безопасности информации. Источники, действия которых могут привести к нарушению безопасности информации, могут быть как внешними, так и внутренними [19].

К внешним источникам угроз относятся следующие группы субъектов:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков телематических услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние источники угроз представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомых с основными функциями и принципами работы программно-аппаратных средств защиты информации, имеющих возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал;
- представители службы защиты информации;
- вспомогательный персонал;
- технический персонал.

Данная группа источников угроз наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить и спрогнозировать [6].

Техногенные источники угроз менее прогнозируемы, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внешними, так и внутренними [19].

К внешним относятся следующие источники угроз:

- средства связи;
- сети инженерных коммуникации;
- транспорт.

Внутренние источники угроз включают в себя следующие группы:

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства;
- другие технические средства, применяемые в учреждении.

Стихийные источники объединяют обстоятельства, составляющие непреодолимую силу, то есть стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить, а также обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры против них должны применяться всегда. Стихийные источники являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы [18, 19]:

- пожары;
- землетрясения;
- наводнения;
- ураганы;
- различные непредвиденные обстоятельства;
- необъяснимые явления;
- другие форс-мажорные обстоятельства.

Классификация источников угроз, проведённая по рассмотренным выше признакам, представлена на рисунке 3.

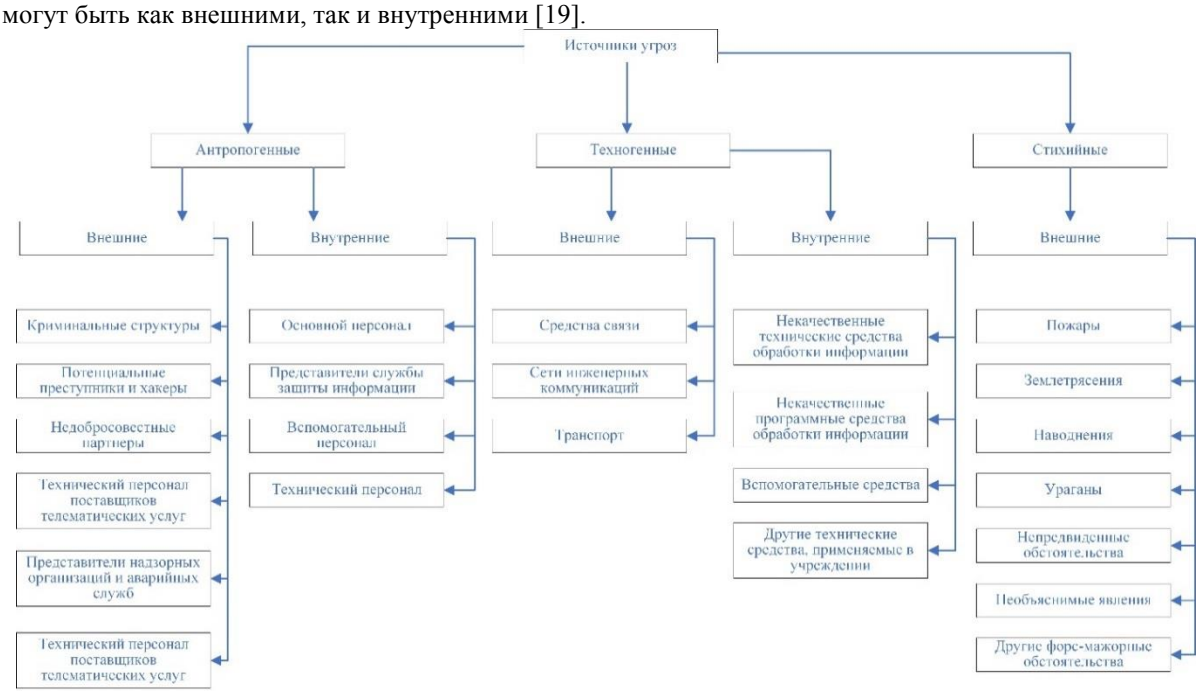

Рисунок 3 – Классификация источников угроз

Источники угроз используют уязвимости для нарушения безопасности информационных систем с целью получения незаконной выгоды. Кроме того, возможны действия источников угроз по активизации тех или иных уязвимостей, не связанные со злым умыслом. Уязвимости информационной системы (ИС) можно разделить по трём признакам [5]:

- по области происхождения;
- по типу недостатков ИС;
- по месту возникновения.

Уязвимости ИС по области происхождения подразделяются на следующие классы [5]:

- уязвимости кода;
- уязвимости конфигурации;
- уязвимости архитектуры;
- организационные уязвимости;
- многофакторные уязвимости.

Уязвимости кода – уязвимости, появившиеся в процессе разработки программного обеспечения.

Уязвимости конфигурации – уязвимости, появившиеся в процессе задания параметров настройки программного обеспечения и технических средств ИС, сети и объектов информатизации.

Уязвимости архитектуры – уязвимости, появившиеся в процессе проектирования ИС, сети или объекта информатизации.

Организационные уязвимости – уязвимости, которые появляются в связи с отсутствием организационных мер защиты информации в ИС и несоблюдением правил эксплуатации системы защиты информации ИС, требований организационно-распорядительных документов по защите информации и несвоевременном выполнении соответствующих действий должностным лицом или подразделением, ответственными за защиту информации [10].

Многофакторные уязвимости – уязвимости, обусловленные наличием в программном обеспечении (ПО) уязвимостей различных классов [3].

Уязвимости ИС по типам недостатков ИС подразделяются на следующие классы [5]:

- неправильная настройка параметров ПО;
- неполнота проверки входных данных;
- возможность прослеживания пути доступа к каталогам;
- возможность перехода по ссылкам;
- возможность внедрения команд операционной системы (ОС);
- межсайтовый скриптинг;
- внедрение интерпретируемых операторов языков программирования;
- внедрение произвольного кода;
- переполнение буфера памяти;
- неконтролируемая форматная строка;
- вычисления;
- раскрытие информации ограниченного доступа;
- управление учетными данными;
- управление доступом;
- аутентификация;
- криптографические преобразования;
- подмена межсайтовых запросов;
- управление ресурсами.

Неправильная настройка параметров ПО заключается в отсутствии необходимого параметра, присвоении параметру неправильных значений, наличии избыточного числа параметров или неопределенных параметров ПО [5]. Примером неправильной настройки ПО является наличие простых паролей доступа к ресурсам ИС, а также наличие в системе незаблокированных встроенных учетных записей пользователей, при помощи которых потенциальный злоумышленник может собрать информацию, необходимую для проведения атаки [12].

Уязвимости, связанные с неполнотой проверки входных данных, могут возникать в случаях, когда вводимые пользователем данные без достаточного контроля передаются интерпретатору некоторого внешнего языка. В этом случае пользователь может задать входные данные так, что запущенный интерпретатор выполнит совсем не ту команду, которая предполагалась авторами уязвимой программы [11].

Прослеживание пути доступа к каталогам заключается в отслеживании пути доступа к каталогу (по адресной строке/составному имени) и получении доступа к предыдущему/корневому месту хранения данных.

Переход по ссылкам связан с возможностью внедрения нарушителем ссылки на сторонние ресурсы, которые могут содержать вредоносный код. Для файловых систем недостатками являются символьные ссылки и возможности прослеживания по ним нахождения ресурса, доступ к которому ограничен.

Внедрение команд ОС заключается в возможности выполнения пользователем команд ОС, например, просмотр структуры каталогов, копирование, удаление файлов и другие команды.

Межсайтовый скриптинг обычно распространен в веб-приложениях и позволяет внедрять код в веб-страницы, которые могут просматривать нелегитимные пользователи. Примерами такого кода являются скрипты, выполняющиеся на стороне пользователя.

Интерпретируемый язык программирования отличается тем, что исходный код не преобразовывается в машинный для непосредственного выполнения центральным процессором, а исполняется с помощью специальной программы-интерпретатора [20]. Часто уязвимость скрывается не в коде приложения, а в программе-интерпретаторе, что является результатом более серьезных проблем с безопасностью в языках программирования.

Внедрение произвольного кода может привести к нарушению процесса выполнения операций.

Переполнение буфера памяти возникает из-за отсутствия контроля за выходом за пределы массива в памяти во время выполнения программы. Когда слишком большой пакет данных переполняет буфер ограниченного размера, содержимое посторонних ячеек памяти перезаписывается, и происходит сбой и аварийный выход из программы [11].

Ошибки форматных строк возникают из-за недостаточного контроля параметров при использовании функций форматного ввода-вывода стандартной библиотеки языка Си. Эти функции принимают в качестве одного из параметров символьную строку, задающую формат ввода или вывода последующих аргументов функции. Если пользователь сам может задать вид форматирования, то эта уязвимость может возникнуть в результате неудачного применения функций форматирования строк [11].

К недостаткам, связанным с вычислениями, относятся следующие:

- некорректный диапазон, когда ПО использует неверное максимальное или минимальное значение, которое отличается от верного на единицу в большую или меньшую сторону;
- ошибка числа со знаком, когда нарушитель может вводить данные, содержащие отрицательное целое число, которые программа преобразует в положительное нецелое число;
- ошибка усечения числа, когда часть числа отсекается;
- ошибка индикации порядка байтов в числах, когда в ПО смешивается порядок обработки битов, что приводит к неверному числу в содержимом, имеющем критическое значение для безопасности.

Раскрытие информации ограниченного доступа, может возникнуть вследствие наличия ошибок, связанных с использованием программ, разработчик которых неизвестен.

Примером недостатков, связанных с управлением учетных данных, может служить нарушение политики разграничения доступа либо ошибки при удалении неиспользуемых учетных данных.

К недостаткам, связанным с аутентификацией, относятся возможность обхода аутентификации, ошибки логики процесса аутентификации, отсутствие запрета множественных неудачных попыток аутентификации и отсутствие требования аутентификации для выполнения критичных функций.

К недостаткам, связанным с криптографическими преобразованиями, относятся ошибки хранения информации в незашифрованном виде, ошибки при управлении ключами и использование несертифицированных средств криптографической защиты информации.

Подмена межсайтового запроса заключается в том, что используемое ПО не может осуществить проверку правильности формирования запроса.

К недостаткам управления ресурсами относятся недостаточность мер освобождения выделенных участков памяти после использования, что приводит к сокращению свободных областей памяти, и отсутствие очистки ресурса и процессов от сведений ограниченного доступа перед повторным использованием.

Уязвимости ИС по месту возникновения подразделяются на следующие классы [5]:

- общесистемное ПО;
- прикладное ПО;
- специальное ПО;
- технические средства;
- портативные технические средства;
- сетевое оборудование;
- средства защиты информации.

К уязвимостям в общесистемном ПО относятся уязвимости ОС, уязвимости систем управления базами данных, а также уязвимости иных типов общесистемного ПО.

К уязвимостям в прикладном ПО относятся уязвимости офисных пакетов программ и иных типов прикладного ПО.

К уязвимостям в специальном ПО относятся уязвимости ПО, разработанного для решения специфических задач конкретной ИС.

К уязвимостям в технических средствах относятся уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода и уязвимости ПО контроллеров управления, интерфейсов управления.

К уязвимостям в портативных технических средствах относятся уязвимости ОС мобильных (портативных) устройств, уязвимости приложений для получения с мобильного устройства доступа к Интернет-сервисам и уязвимости интерфейсов беспроводного доступа.

К уязвимостям в сетевом оборудовании относятся уязвимости маршрутизаторов, коммутаторов, концентраторов, мультиплексоров, мостов и телекоммуникационного оборудования.

К уязвимостям в средствах защиты информации относятся уязвимости в средствах управления доступом, средствах идентификации и аутентификации, средствах контроля целостности, средствах доверенной загрузки, средствах антивирусной защиты, системах обнаружения вторжений, средствах межсетевого экранирования, средствах управления потоками информации, средствах ограничения программной среды, а также средствах стирания информации и контроля удаления информации [5].

В таблице 1 соотнесены группы источников угроз с уязвимостями информационной системы.

Таблица 1

Соотношение источников угроз с уязвимостями информационной системы

Источник угрозы	Уязвимость
Антропогенные источники угроз	Уязвимости кода
	Уязвимости конфигурации
	Уязвимости архитектуры
	Организационные уязвимости
	Многофакторные уязвимости
	Неправильная настройка параметров ПО
	Неполнота проверки входных данных
	Возможность прослеживания пути доступа к каталогам
	Возможность перехода по ссылкам
	Возможность внедрения команд ОС
	Межсайтовый скриптинг
	Внедрение произвольного кода
Техногенные источники угроз	Внедрение интерпретируемых операторов языков программирования
	Переполнение буфера памяти
	Ошибки форматных строк
	Вычисления
	Аутентификация
	Криптографические преобразования
	Управление ресурсами
	Общесистемное ПО
	Прикладное ПО
	Специальное ПО
	Технические средства
	Портативные технические средства
	Сетевое оборудование
	Средства защиты информации

В заключение можно отметить, что такая классификация компьютерных сетей, сетевых атак, источников угроз, а также уязвимостей ИС, достаточно полно отражает представление об имеющихся их видах, что позволяет минимизировать потенциальный ущерб, который может быть нанесён ИС.

Список литературы

1. Атака «man in the middle» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/.

2. Атака канального уровня ARP-spoofing и как защитить коммутатор Cisco [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/192022/.

3. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/ubi/terms/terms/view/id/26.

4. Виды компьютерных атак [Электронный ресурс]. – Режим доступа: https://kompkimi.ru/programms-2/sistemnye-programmy/zashhita-pk/vidy kompyuternyx-atak#i.

5. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200123702.

6. Интернет-издание о высоких технологиях [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class. shtml.

7. Классификация по типу среды передачи [Электронный ресурс]. – Режим доступа: https://sites.google.com/site/makeevainftechkomputernyeseti/home/klas sifikazia/sreda.

8. Классификация сетевых атак [Электронный ресурс]. – Режим доступа: https://helpiks.org/8-55790.html.

9. Классификация сетевых атак [Электронный ресурс]. – Режим доступа: https://studbooks.net/2261861/informatika/klassifikatsiya_setevyh_atak.

10. Лаборатория центра информационной и общественной безопасности [Электронный ресурс]. – Режим доступа: http://lab.infosec.uz/site/info-vul.

11. Поиск уязвимостей в программах с помощью анализаторов кода [Электронный ресурс]. – Режим доступа: http://www.codenet.ru/progr/other/code-analysers.php.

12. Сердюк, В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах: уч. издание/ В.А. Сердюк. – М: Издательский дом НИУ ВШЭ, 2011 – 576 с.

13. Сети передачи данных [Электронный ресурс]. – Режим доступа: https://zametkinapolyah.ru/kompyuternye-seti/tipy-kompyuternyx-setej.html.

14. Сети хранения данных [Электронный ресурс]. – Режим доступа: http://www.starlink.ru/articles/storage-networks/.

15. Типы компьютерных сетей [Электронный ресурс]. – Режим доступа: http://informatics-lesson.ru/net/type-net.php.

16. Типы компьютерных сетей [Электронный ресурс]. – Режим доступа: http://itandlife.ru/technology/computer-networks/tipy-kompyuternyx-setej-klassifikaciya-kompyuternyx-setej/.

17. Типы компьютерных сетей и способы их управления [Электронный ресурс]. – Режим доступа: http://lanfix.ru/clauses/tipy-kompjuternyh-setej-i-sposoby-ih-upravlenija/.

18. Угрозы безопасности для информационной системы [Электронный ресурс]. – Режим доступа: http://www.security.ase.md/publ/ru/pubru91/.

19. Угрозы информационной безопасности [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности.

20. Уязвимости в популярных языках программирования [Электронный ресурс]. – Режим доступа: https://www.itweek.ru/security/article/detail.php?ID=199013.