Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

СПРАВОЧНИК ТЕРМИНОВ И ЖАРГОНИЗМОВ ДЛЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Справочник

Москва

Московский университет
МВД России имени В.Я. Кикотя

2022

УДК 004.9
ББК 16.8
С74

Рецензенты:
начальник кафедры УОРП Академии управления МВД России
доктор юридических наук, доцент **Ю. В. Гаврилин;**
старший оперуполномоченный ОУР УВД по СВАО
ГУ МВД России по г. Москве **П. Д. Лопатин**

Коллектив авторов:
И. Г. Чекунов, А. В. Пузарин, В. В. Гончар,
И. А. Рядовский, Р. Р. Сабитов, Н. Е. Клишина, Д. В. Галиев

С74 **Справочник терминов и жаргонизмов для расследования преступлений в сфере информационных технологий** : справочник / [И. Г. Чекунов и др.]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2022. – 105 с.
ISBN 978-5-9694-1173-9

Справочник состоит из материалов и терминов, выработанных в результате совместной работы специалистов «Лаборатории Касперского», сотрудников Московского университета МВД России имени В.Я. Кикотя и Следственного департамента МВД России.

УДК 004.9
ББК 16.8

ISBN 978-5-9694-1173-9

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Четвертая промышленная революция, сопровождающаяся цифровой трансформацией различных сфер общественной жизни, создает значительные преимущества для потребителей различных услуг, увеличивает качество, скорость, доступность получения гражданами различных электронных сервисов, совершенствуются различные сферы общественной жизни и бизнес-модели функционирования организаций. Новые технологии и возможности создают дополнительные риски: так, увеличивается вероятность эксплуатации сети Интернет для совершения противоправных действий.

В настоящее время отмечается высокая латентность таких противоправных действий, во многом обусловленная возможностью преступников оставаться анонимными, избегать непосредственного контакта с потерпевшими, широкой аудиторией пользователей информационных ресурсов, упрощением доступа к этим ресурсам, а также организованным и трансграничным характером подобных деяний.

В связи с ростом количества преступлений рассматриваемой категории и появлением новых вариативных методов, способов и средств их совершения возникла необходимость подготовки справочника терминов и жаргонизмов для расследования преступлений в сфере информационных технологий.

ГЛАВА 1. ЦИФРОВЫЕ ДАННЫЕ – DIGITAL DATA

Информация (англ. Information) – сведения (сообщения, данные) независимо от формы их представления [1].

Данные (англ. Data) – информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека [12].

Цифровые данные (англ. Digital data) – данные, представленные в виде набора цифровых сигналов. В современной вычислительной технике данные представляются в виде двоичных чисел, т. е. в виде 0 и 1 (да или нет, истина или ложь).

Вычислительное устройство (компьютер, англ. Computing device) – устройство, способное передавать, обрабатывать и хранить цифровые данные. Вычислительное устройство может быть компьютером в бытовом понятии (ПК) или содержаться в различных устройствах: пластиковые карты, гаджеты (фитнес-браслеты, умные часы), бытовая техника – от электрочайника до холодильника (см. Интернет вещей) и т. д.

Единицы измерения информации

Бит (англ. Bit) – минимальная единица измерения информации в двоичной системе счисления. Может принимать только два значения – 1 и 0 (истина и ложь – англ. True и False).

Байт (англ. Byte) – единица измерения информации, равная (в современных системах) 8 бит. Может принимать 256 различных значений (от 0 до 255). Пример: десятичное число 209 может быть представлено в двоичной системе как 11010001. 1 024 байт равны 1 килобайт (сокр. Кбайт (Кб), Kbyte (KB), в свою очередь, 1 024 килобайт равны 1 мегабайт (сокр. Мбайт (Мб), Mbyte (MB), 1 024 мегабайт – 1 гигабайт (сокр. Гбайт (Гб), Gbyte (GB), 1024 гигабайт – 1 терабайт (сокр. Тбайт (Тб), Tbyte (TB) и т. д.

Стоит учитывать, что для измерения скорости передачи данных используются биты, килобиты (равный 1 000 бит, сокр. Кбит, Kbit), мегабиты (1 000 Кбит, сокр. Мбит, Mbit) и гигабиты (1 000 Мбит, сокр. Гбит, Gbit) в секунду. Также производители накопителей данных указывают объем накопителя в десятичной системе счисления: 1 Кбайт равен 1 000 байт, 1 Мбайт равен 1 000 Кбайт и т. д.

Октет (англ. Octet) – единица измерения информации, равная 8 битам (см. Байт).

Примечание. Термин «октет» может применяться вместо «байта», так как «байт» может содержать количество битов, отличное от восьми. Пример: IP-адреса (ipv4) записываются как четыре «октета» (целые числа от 0 до 255), разделенные точкой: 192.168.0.255.

Кодирование данных – Data encoding

Кодирование данных (англ. Encoding) – обратимое преобразование данных по определенному алгоритму из одного представления (записи) в другое.

Примечание. Не стоит путать кодирование с шифрованием: оба делают обратимое преобразование, однако целью кодирования является не сокрытие данных, а приведение в пригодный для их хранения и передачи вид.

Существует деление на **текстовые** (англ. plain text) и **двоичные (бинарные)** (англ. binary) данные. Текстовые данные состоят только из читабельных (печатных) символов и управляющих символов. В свою очередь, бинарными данными называют все то, что нельзя отнести к текстовым данным (*рис. 1*).

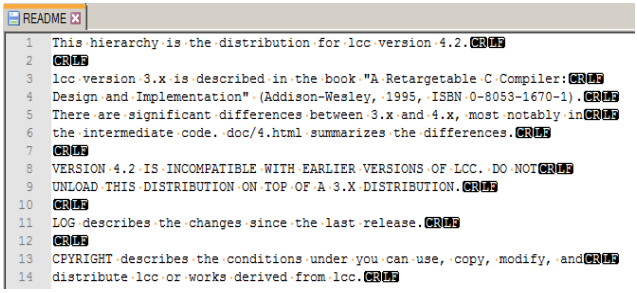

Рис. 1. Пример текстового файла. Для наглядности отображены управляющие символы (переноса каретки и новой строки – CR и LF)

Управляющие символы (англ. Control character) – специальные символы, используемые при кодировании текстовых данных (например, ASCII или ANSI), которые не отображаются и указывают на определенное действие (управление устройством вывода, цвет текста и т. д.). Примеры управляющих символов: перевод строки («\n», код символа 0x0A, англ. Line Feed (LF), возврат каретки («\r», код символа 0x0D, англ. Carriage Return (CR), знак табуляции (\t).

Бинарный (двоичный) файл (сленг «бинарь»/«бинарник», англ. Binary file) – файл, частично или полностью состоящий из двоичных данных. «Бинарь» может содержать и текстовые символы. Например, «бинарь» может называться «архив», «зашифрованный файл», «исполняемый (машинный) код» или «шелл-код», «случайная последовательность», «байт» (*рис. 2*).

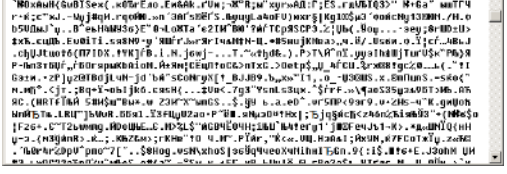

Рис. 2. Пример бинарного файла, открытого в текстовом редакторе. Файл содержит много нечитаемых символов

Нулевой байт (сленг «нулл-байт», англ. Null byte) – байт, равный 0 (в шестнадцатеричной записи – 0x00).

Шестнадцатеричная система счисления (сленг «хекс», англ. hexadecimal (hex) – позиционная система счисления по целочисленному основанию 16.

В качестве цифр этой системы счисления обычно используются цифры от 0 до 9 и буквы латинского алфавита от A до F. Например, числа с различными приставками («0x», «h», «\x»), указывающими на шестнадцатеричное представление, – 0x19, FA30DEh, \x1B\x00.

Шестнадцатеричный редактор, **Hex-редактор** («хекс-редактор», англ. Hex-editor) – программа, позволяющая отображать содержимое файлов (в первую очередь, бинарных) в шестнадцатеричном представлении (значение каждого байта представлено в виде шестнадцатеричного числа), а также позволяющая редактировать их содержимое (*рис. 3*).

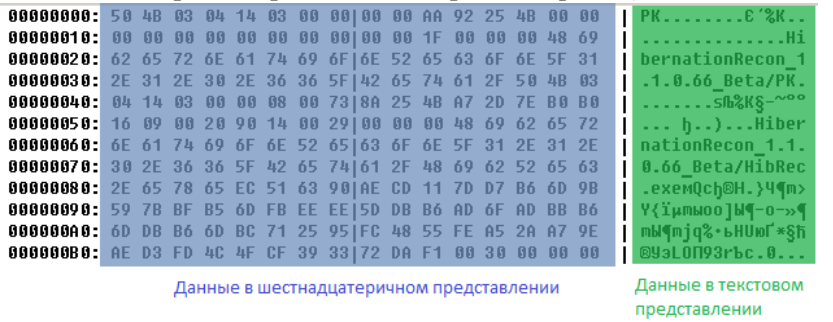

Рис. 3. Пример части файла (zip-архив), открытого в шестнадцатеричном редакторе (hex-редактор). Содержимое начала файла дано в двух представлениях: шестнадцатеричном и текстовом виде (ANSI)

MIME («майм», англ. Multipurpose internet mail extensions) – стандарт, описывающий правила кодирования различных типов данных (текст на произвольном языке, аудио-, видеоизображения, программы и т. д.) в текстовом виде для пе-

редачи по вычислительным сетям (в первую очередь, посредством электронной почты и HTTP-протокола).

Base64 (кодирование по основанию 64, сленг «бейс») – алгоритм преобразования двоичных (бинарных) данных в текстовое представление. Алгоритм кодирует данные в набор из 64 печатных символов (алфавит): большие и маленькие латинские буквы, цифры и два дополнительных символа, в зависимости от версии кодировки (для стандарта MIME используются символы «+» и «/»), для выравнивания до нужной длины могут добавляться «=» в конце закодированной строки. Например, «dGVzdCB0ZXh0XCE=» является строкой «test text!», закодированной по алгоритму Base64. По аналогии с Base64 кодирование двоичных данных может осуществляться по другому основанию (количеству символов), например менее распространенные алгоритмы Base58 и Base91 используют для кодирования 58 и 91 символ соответственно.

QR-код («кью-ар-код», англ. QR-code) – вид машиночитаемого кода, двухмерный аналог штрих-кода (*рис. 4*).

Рис. 4. Пример текста «test text», закодированного в QR-коде

Сериализация (англ. Serialization) – процесс преобразования структуры данных в формат, пригодный для хранения и передачи. Обратный процесс – десериализация. Пример: JSON, XML, YAML – текстовые форматы для хранения и обмена информацией, доступной для чтения человеком.

12

JSON:

```
{
  "firstName": "Иван",
  "lastName": "Иванов",
  "address": {
    "streetAddress": "Московское ш., 101, кв. 101",
    "city": "Ленинград",
    "postalCode": 101101
  },
  "phoneNumbers": [
    "812 123-1234",
    "916 123-4567"
  ]
}
```

XML:

```
<person firstName="Иван" lastName="Иванов">
  <address streetAddress="Московское ш., 101, кв. 101"
city="Ленинград" postalCode="101101" />
  <phoneNumbers>
    <phoneNumber>812 123-1234</phoneNumber>
    <phoneNumber>916 123-4567</phoneNumber>
  </phoneNumbers>
</person>
```

YAML:

```
--- # The Smiths
- {name: John Smith, age: 33}
- name: Mary Smith
  age: 27
- [name, age]: [Rae Smith, 4]   # sequences as keys are supported
--- # People, by gender
```

men: [John Smith, Bill Jones]
women:
- Mary Smith
- Susan Williams

Представление даты и времени

Временная метка (сленг «таймстамп», англ. Timestamp) – время, в которое было отмечено (записано) некоторое событие. Например, временная метка создания файла, временная метка подключения, временная метка доступа к ресурсу по протоколу http в журнале access.log веб-сервера. Временная метка может быть подделана, в частности, утилитами timestomp и touch (файл «потачен»).

UNIX-время (англ. Unix time) – формат хранения времени, представленный в виде количества секунд с полуночи 1 января 1970 г. в часовом поясе UTC. Пример: 1 398 120 304 соответствует 22 часам 45 минутам и 4 секундам 21 апреля 2014 г. по UTC.

Всемирное координированное время (UTC) (англ. Coordinated universal time) – основной стандарт определения времени и даты. UTC пришел на смену устаревшему среднему времени по Гринвичу (GMT), разница между которыми может достигать одной секунды. UTC не учитывает переход на летнее время. Часовые пояса обозначаются как смещение относительно UTC, например, московское время (МСК, MSK) соответствует UTC+3.

Сервер точного времени (англ. Time server) – сетевой узел, предоставляющий информацию о текущем времени другим сетевым узлам. Для синхронизации времени используется сетевой протокол NTP (англ. Network time protocol).

Накопители данных – Data storage

Машинный носитель (данных) – сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах [13].

Жесткий диск (накопитель на жестких магнитных дисках (НЖМД), сленг «хард», «винт»/«винч» от устар. «винчестер», англ. Hard disk drive (HDD) – основной накопитель данных, содержащий вращающиеся на шпинделе магнитные диски (сленг «блины»), данные с которых считываются и записываются с помощью подвижных головок. НЖМД чувствительны к механическим воздействиям. Распространенными интерфейсами для подключения НЖМД являются параллельный IDE/ATA (устаревший интерфейс), последовательный SATA (наиболее часто встречается) и SAS (используется в серверных системах).

Твердотельный накопитель (сленг «ссд», англ. Solid-state drive (SSD) – пришедший на смену НЖМД накопитель данных, использующий микросхемы для хранения данных. По сравнению с НЖМД твердотельные накопители быстрее, меньше по размерам, бесшумны и устойчивы к механическим воздействиям (*рис. 5*).

Рис. 5. Внешний вид НЖМД (HDD) – слева,
вид твердотельного накопителя (SSD) – справа

Оптический диск (устар. «компакт-диск», англ. Optical disk) – накопитель данных в виде пластмассового диска с посадочным отверстием, чтение (и запись) данных с которого производится посредством лазера в приводе оптических дисков (англ. Optical disk drive). Распространены следующие типы оптических дисков: CD (емкость 700–900 Мб), DVD (емкость от 4 812 до 17 408 Мб), BlueRay (емкость от 25 600 Мб). Оптические диски могут быть только на чтение (записанные на заводе), с однократной записью (CD-R, DVD-R, DVD+R) и перезаписываемыми (CD-RW, DVD-RW, DVD+RW). Также обозначение DL (англ. Dual layer) у DVD обозначает двухслойный накопитель с увеличенным объемом. Чистый диск, пригодный для записи, называют «болванкой».

Внешний (съемный) накопитель (англ. Removable storage device) – накопитель данных, который можно легко извлечь и переместить с одного устройства на другое. Например, к таким накопителям относятся оптические диски, внешние жесткие диски и USB-накопители. Внешний накопитель, с которого может загружаться ОС (так называемый Live-дистрибутив ОС, который не требует установки на НЖМД), называется загрузочным (англ. Boot disk).

USB-накопитель, **Флеш-накопитель** (USB-флеш-накопитель, сленг «флешка», англ. USB flash drive) – портативный накопитель данных, использующий флеш-память (полупроводниковая технология).

Карта памяти (англ. Memory card) – компактный носитель данных в виде пластиковой карты. Используется в портативных устройствах, в частности в телефонах и фотоаппаратах. Примеры: SD, MicroSD, Memory Stick.

Сетевое хранилище, **Сетевая система хранения данных** (сленг «нас», англ. Network attached storage (NAS) – устройство, предназначенное для хранения большого объема данных, до-

ступ к которым осуществляется по сети. Для хранения данных обычно используется несколько НЖМД, объединенных в RAID.

RAID («рейд», англ. Redundant array of independent disks) – технология, позволяющая объединять несколько накопителей данных в логическую единицу в целях повышения надежности и производительности, которые достигаются за счет избыточности – данные хранятся одновременно на нескольких носителях. Основные схемы объединения накопителей (уровни): RAID 0 – распределенное хранение данных без избыточности, RAID 1 («зеркалирование») – накопители являются копиями друг друга, RAID 10 – комбинация из RAID 0 и RAID 1, RAID 5 – распределенное хранение данных, при котором может выйти из строя один накопитель, RAID 6 – аналогично RAID 5, но могут выйти из строя два накопителя.

Сектор диска (англ. Disk sector) – минимальная адресуемая единица хранения данных на дисковых накопителях. Стандартный размер сектора НЖМД – 512 байт, на оптических дисках – 2 048 байт, на современных НЖМД – 4 096 байт (расширенный формат).

Логический раздел (сленг «партиция», англ. Partition) – логическая область носителя информации, выделенная пользователем для определенной цели, например для хранения данных. Разделы, содержащие необходимые для загрузки ОС файлы и непосредственно ОС, называются **загрузочным** (англ. System partition) и **системным** (англ. Boot partition) разделами соответственно. Системный раздел может быть одновременно загрузочным. Для ОС семейства Microsoft Windows разделом, содержащим систему, обычно является «диск С», однако в терминах Microsoft данный раздел называется загрузочным.

Том (логический диск, англ. Volume, Logical drive) – единая область хранения данных с одной файловой системой. Обычно том находится на одном разделе накопителя данных, однако накопитель может вовсе не содержать логических раз-

делов (например, оптический диск или флеш-накопитель) и восприниматься ОС как один том. В то же время один том может располагаться в нескольких разделах разных накопителей.

Менеджер логических томов (LVM, англ. Logical Volume Manager) – подсистема ОС Linux, абстрагирующая расположение логических томов на физических носителях данных. Например, благодаря LVM один логический том может располагаться на нескольких НЖМД и изменять размер тома без потери данных.

MBR (англ. Master boot record) – главная загрузочная запись размером 512 байт, которая находится в самом начале НЖМД или любого другого загрузочного накопителя. Содержит информацию о четырех первичных логических разделах НЖМД (в устаревшем формате – CHS (цилиндр, головка, сектор), а также 16-разрядный исполняемый код, запускаемый BIOS, который выбирает загрузочный логический раздел и передает управление VBR этого раздела. Для хранения исполняемого кода MBR могут дополнительно использоваться несколько секторов после первых 512 байт.

VBR (англ. Volume Boot Record) – загрузочная запись логического раздела размером 512 байт, которая находится в самом начале логического раздела. Предназначена для поиска файлов и начальной загрузки ОС. Для хранения исполняемого кода VBR могут дополнительно использоваться несколько секторов после первых 512 байт.

GPT (англ. GUID Partition Table) – современная альтернатива MBR, используемая совместно с EFI. Применяет современную адресацию логических блоков и дублирование (таблица разделов хранится в начале и конце НЖМД).

Файловая система – File system

Файл (англ. File) – именованная совокупность данных. Характеризуется именем файла, которое может содержать (в част-

ности, в ОС семейства Microsoft Windows) расширение файла, отделенное точкой от имени файла.

Файловая система (ФС) (англ. File system) – это структура и порядок физического расположения данных (информации) на его носителе в виде объектов файловой системы как: файл, каталог, символьные ссылки и т. д. Пример: NTFS, FAT32, exFAT, ext4, HFS+, APFS.

Сетевая файловая система (англ. Network file system) – файловая система, взаимодействие с которой происходит по сети (см. NFS).

Каталог (папка, директория, англ. Directory, Folder) – с точки зрения пользователя – это именованный объект файловой системы, способный содержать подобные себе объекты (файлы и другие каталоги).

Корневой каталог (корень файловой системы, сленг «рут», англ. Root) – основной (верхний) каталог в иерархии файловой системы, в котором располагаются все остальные файловые объекты.

Путь (англ. Path) – адрес, указывающий на расположение объекта файловой системы (файла, каталога). Путь может быть абсолютным (полным) – указывающим на объект, начиная с корня файловой системы (путь начинается с «/»), либо относительным – указывающим относительно текущего каталога (путь начинается с «./» или «../») или домашнего каталога пользователя («~/»). В ОС семейства Microsoft Windows путь обозначается через обратную косую черту «\» (сленг «бекслеш», англ. Backslash), в то время как в Unix-подобных ОС используется косая черта «/» (сленг «слеш», англ. Slash). Пример: абсолютный путь до файла – «C:\Windows\System32\drivers\etc\hosts», абсолютный путь до каталога – «/usr/share/nmap/scripts/», путь относительно домашнего каталога – «~/Library/Application Support/Google/Chrome/».

Монтирование (англ. Mount) – процесс присоединения файловой системы (с логического раздела, образа или сетевого

ресурса). После она становится доступна пользователю по определенному пути, называемому точкой монтирования (англ. Mount point). Обратный процесс называют размонтированием (англ. Unmount).

Формат файла (англ. File format) – логическая структура хранения данных в файле. Указанная структура может содержать метаданные, в частности «заголовок» (сленг «хедер» (англ. Header), располагаемый обычно в начале файла и содержащий информацию о файле. Также на формат файла могут указывать характерные сигнатуры (так называемые магические числа, англ. Magic number). Пример: графические файлы в формате GIF в начале файла содержат строку «GIF89a».

Расширение файла (англ. Filename extension) – символьное обозначение формата файла, располагаемое после основного имени файла и отделяемое от него точкой. Пример: имя файла «linux-4.7.5.tar.gz» состоит из основного имени файла «linux-4.7.5» и расширения «tar.gz», указывающего на тип файла (архив).

Атрибуты файла (свойства файла, англ. File attributes, File properties) – характеристики файла, определяемые ОС и прикладным ПО [20]. Атрибуты файла не содержатся в самом файле, а являются метаданными, поддерживаемыми ОС.

Метаданные (англ. Metadata) – данные, содержащие дополнительные сведения об объекте. Например, метаданные файла могут содержать информацию о владельце, правах доступа, дате создания, модификации файла и т. д.

Символическая ссылка (сленг «симлинк», англ. Symbolic link, symlink) – объект файловой системы (специальный файл), указывающий на другой объект (файл или каталог).

Ярлык (англ. Shortcut) – файл, указывающий на другой объект файловой системы, сетевой ресурс или ПО. В ОС семейства Microsoft Windows ярлыки имеют расширение файла «.lnk» и «.url».

Временный файл (сленг «темп», англ. Temporary file, tempfile) – файл, создаваемый программой на ограниченное время [4]. Время хранения файла определяется ОС. Обычно, но не всегда, временные файлы удаляются при перезагрузке.

Архивирование (англ. Archiving) – преобразование данных в компактную форму без потери содержащейся в них информации с помощью специализированной программы в целях экономии места на носителе информации и (или) повышения эффективности передачи данных [4].

Архивный файл (сленг «архив», англ. Archive file) – файл, полученный в результате архивирования одного или нескольких файлов [4]. Пример форматов: Zip, tar, 7-Zip, RAR.

Разархивирование (англ. Unpack) – извлечение файлов из архивного файла [4].

Заполнитель файлового пространства (англ. File slack space) – пространство между концом файла и концом кластера файловой системы.

Обработка данных – Data processing

Синтаксический анализ (разбор, сленг «парсинг», англ. Parsing) – процесс анализа набора символов (строковых данных), содержащих естественный или формальный язык либо структуру данных, согласно правилам формальной грамматики. Пример: «парсить» веб-страницу для того, чтобы получить указанные в ней адреса электронной почты. Для «парсинга» могут применяться регулярные выражения.

Регулярные выражения (сленг «регулярка», «регэксп», англ. Regular expressions (RegExp) – формальный язык в виде последовательности символов, описывающий шаблон (паттерн, маску), по которому производится поиск строковых данных.

Форматы данных – Data formats

XML (англ. eXtensible markup language) – язык разметки, определяющий набор правил для представления данных в форме, пригодной для восприятия как человеком, так и вычислительным устройством.

JSON (англ. JavaScript object notation) – текстовый формат представления произвольных данных. Данные в формате JSON часто применяются для взаимодействия программ между собой (см. API).

CSV (англ. Comma-separated values) – простой текстовый формат, предназначенный для хранения табличных данных, где данные столбцов разделяются запятыми или другим разделителем, например знаком табуляции CSV – TSV.

ГЛАВА 2. ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА – COMPUTING DEVICES

Аппаратное обеспечение – Hardware

Аппаратное обеспечение (сленг «железо», англ. Hardware) – любое физическое устройство, осуществляющее обработку данных [14].

Средство вычислительной техники (СВТ) – совокупность технических устройств и программ, обеспечивающих их функционирование, способных работать самостоятельно или в составе других систем [4].

Форм-фактор (типоразмер, англ. Form factor) – обобщенное название для стандарта, задающего характерные физические параметры устройства (материнской платы, накопителя данных, корпуса и т. д.), такие как габариты устройства (изделия), его форма, расположение отверстий и т. д.

Системный блок (сленг «системник», англ. Computer case) – корпус (шасси), в котором располагаются основные компоненты вычислительного устройства (компьютера), такие как блок питания, материнская плата с центральным процессором и оперативной памятью, видеокарта, накопители данных, платы расширения, привод оптических дисков и т. д.

Моноблок – системный блок и монитор в одном корпусе.

Периферийное оборудование – совокупность технических средств и ПО, предназначенная для взаимодействия центрального процессора с внешней средой и для хранения информации [13].

Материнская плата (сленг «мать», «материнка», англ. Motherboard) – основная электронная плата вычислительного устройства, на которой размещаются его ключевые компоненты: центральный процессор, оперативная память, ПЗУ, слоты расширения и т. д.

Оперативная память (сленг «оперативка», «рам»/«рама», «мозги», устар. «оперативное запоминающее устройство» (ОЗУ), англ. Random-access memory (RAM) – вид памяти, в которой хранится выполняемый машинный код (программы) и обрабатываемые им данные.

Примечание. Оперативная память является энергозависимой, т. е. хранит данные только при наличии электрического питания.

ПЗУ (постоянное запоминающее устройство, англ. Read-only memory (ROM) – энергонезависимая память, хранящая данные, доступные только для чтения.

BIOS («биос», англ. Basic input/output system) – микропрограмма, отвечающая за контроль подключенных устройств, а также обеспечивающая загрузку и работу ОС. BIOS хранится на микросхеме (ПЗУ), которая располагается на материнской плате вычислительного устройства. Для загрузки ОС BIOS использует главную загрузочную запись (MBR). На смену BIOS пришел стандарт **UEFI** (EFI, англ. (Unified) Extensible firmware interface).

Видеокарта (видеоадаптер, сленг «видяха», «видуха», англ. Videocard, Videoadapter) – устройство (обычно выполненное в виде платы расширения), позволяющее выводить изображение на экран (монитор).

Примечание. Современные видеокарты позволяют проводить математические вычисления на графическом процессоре (сленг «гпу», GPU), не связанные с графическими вычислениями. Особенностью графического процессора является большее количество ядер (в несколько сотен раз) по сравнению с центральным процессором (CPU), что удобно для параллельного выполнения вычислений, в частности для майнинга некоторых

видов криптовалют или поиска коллизий в хеш-значениях методом перебора (см. Полный перебор (Brute-force).

Интерфейс (англ. Interface) имеет широкое употребление в нескольких разных значениях. Интерфейс в широком смысле – набор правил взаимодействия объектов. Объекты могут представлять из себя аппаратное и (или) ПО. Интерфейс может означать точку взаимодействия между аппаратным и (или) По наряду с набором правил такого взаимодействия.

Машинный код (англ. Machine code, Machine language) – набор команд (инструкций), выполняемых непосредственно центральным процессором вычислительного устройства.

Перезагрузка (сленг «ребут», «рестарт», англ. Reboot) – процесс перезапуска вычислительного устройства, при котором очищается содержимое оперативной памяти и ОС загружается заново. Выделяют «холодную» («жесткую») перезагрузку – с выключением электрического питания (в том числе по нажатию кнопки «ресет» (англ. Reset) и «горячую» («мягкую») – выполненную программно.

Исполняемый код (англ. Executable code) – код (набор команд), представленный в виде машинного кода, байт-кода или кода, на интерпретируемом (скриптовом) языке.

Байт-код (промежуточный код, англ. Bytecode, Portable code, p-code) – набор аппаратно-независимых инструкций (команд), выполняемых в специальном интерпретаторе байт-кода (виртуальной машине). Позволяет создавать ПО, запускаемое на любом аппаратном обеспечении.

Кэш (англ. Cache) – промежуточный буфер (область памяти), обеспечивающий быстрый доступ к часто запрашиваемым данным.

Кластер (англ. Cluster) – объединение нескольких однородных элементов, которое может рассматриваться как самостоятельная единица, обладающая определенными свойствами

[1]. Пример: кластер серверов, позволяющий объединить вычислительные возможности за счет увеличения количества вычислительных устройств (серверов).

Виртуализация – Virtualization

Виртуализация (англ. Virtualization) – это логическое абстрагирование вычислительных ресурсов от физических ограничений [16]. Одной из типовых абстракций является виртуальная машина. Кроме виртуальных машин виртуализация может выполняться в отношении множества других вычислительных ресурсов, таких как приложения, настольные компьютеры, сети и системы хранения [16].

Виртуальная машина (сленг «виртуалка», англ. Virtual machine) – аппаратное обеспечение, эмулируемое специальным ПО – гипервизором (англ. Hypervisor), обеспечивающее работу «гостевой» ОС (англ. Guest OS), запускаемое в рамках основной «хостовой» (англ. Host) системы. Пример: на «хостовой» ОС Microsoft Windows 7 с применением ПО виртуализации VMware Workstation может быть запущена виртуальная машина под управлением гостевой ОС GNU/Linux.

Снимок (виртуальной машины) (сленг «снепшот» / «снапшот», англ. Snapshot) – зафиксированное в определенный промежуток времени промежуточное состояние, к которому возможно приведение (откат) виртуальной машины.

Контейнеризация (контейнерная виртуализация, англ. Containers) – метод виртуализации, при котором ядро ОС поддерживает несколько изолированных экземпляров пространства пользователя вместо одного. Пример: Docker (сленг «докер»).

Мобильные устройства, встраиваемые системы – Mobile device, Embedded system

Встраиваемая система (встроенная система, англ. Embedded system) – вычислительное устройство, выполняющее определенную функцию внутри другой системы (устройства).

Интернет вещей (англ. Internet of Things (IoT) – концепция сети, объединяющей различные физические устройства, содержащие встраиваемые системы, в частности бытовые приборы.

Гаджет (англ. Gadget) – собирательное название для портативных вычислительных устройств, обычно имеющих конкретное предназначение в быту. Пример: фитнес-браслет, смартфон.

NFC (англ. Near field communication) – технология беспроводной передачи данных на короткие расстояния (порядка 10 см). Устройства NFC могут использоваться для идентификации и применяются для организации бесконтактных платежей.

Оператор сотовой связи (сленг «ОПСОС»).

SIM-карта (сленг «симка», англ. Subscriber identification module) – пластиковая карта, содержащая микросхему, позволяющая в мобильной сети идентифицировать абонента. SIM-карта может быть незаконно перевыпущена (восстановлена) злоумышленниками по поддельной доверенности либо через инсайдера в ОПСОСе.

GPRS (англ. General Packet Radio Service – технология пакетной радиосвязи общего пользования) – служба мобильной связи, доступная пользователям мобильных телефонов GSM. Позволяет эффективно использовать ограниченную полосу пропускания сети. Обычно используется для передачи и получения небольших объемов данных, например для чтения электронной почты или просмотра веб-страниц [16].

GSM (англ. Global system for mobile communications – глобальная система мобильной связи) – популярный стандарт для мобильных телефонов и сетей [16].

IIN (англ. Issuer identification number) – идентификационный номер эмитента (организации, выпустившей идентификационную карту). Для SIM-карты IIN имеет следующий формат: 89 (код индустрии для использования в телекоммуникации) + код страны (1–3 цифры) + код эмитента (1–4 цифры).

ICCID (англ. Intagrated chip card identification) – уникальный идентификатор SIM-карты длиной от 19 до 22 цифр, имеющий следующий формат: IIN + 12 цифр + уникальный номер + контрольная цифра по алгоритму Луна.

IMEI (англ. International Mobile Equipment Identity) – международный идентификатор мобильного оборудования, состоящий из 15 цифр.

MCC (англ. Mobile country code) – трехзначный мобильный код страны. Для России код MCC равен 250.

MNC (англ. Mobile network code) – код мобильной сети длиной две или три цифры. MCC с MNC является уникальным идентификатором оператора связи.

IMSI (англ. International mobile subscriber identity) – международный идентификатор абонента мобильной сети. IMSI состоит из MCC, MNC и уникального идентификатора (MSIN).

MSISDN (англ. Mobile station ISDN number) – номер абонента сети сотовой связи. MSISDN (до 15 цифр) состоит из 1–3 цифр кода страны (для России – 7, англ. Country code, CC), 2–3 цифр национального кода направления (англ. National Destination code, NDC) и номера абонента (англ. Subscriber number, SN).

«Холодный» звонок (сленг «холодильник», «холодник», англ. cold-calling) – телефонный звонок абоненту, который не давал для этого своего согласия.

Звонарь (сленг, сленг «хантер», англ. Hunter) – сотрудник кол-центра, производящий «холодный» обзвон.

Клоузер (сленг, англ. Closer) – получает «холодный» звонок от «хантера», цель которого – завершить «сделку».

USSD (англ. Unstructured supplementary service data) – протокол, используемый в сетях GSM, позволяющий передавать короткие сообщения в реальном времени.

HLR (англ. Home location register) – база данных, которая содержит информацию об абоненте сети GSM-оператора. Посредством HLR-запроса возможно определение доступности абонента и его оператора.

Система сигнализации № 7 (ОКС-7, англ. Common channel signaling, Signaling system 7 (SS-7) – набор сигнальных телефонных протоколов, используемых для настройки большинства телефонных станций. В основе ОКС-7 лежит использование аналоговых или цифровых каналов для передачи данных и соответствующей управляющей информации.

Базовая станция (сленг «сота», англ. Base station) – комплекс радиопередающей аппаратуры (ретрансляторы, приемопередатчики), осуществляющий связь с конечным абонентским устройством – сотовым телефоном.

Фемтосота (англ. Femto access points) – маломощная базовая станция, которая подключена к сети оператора через Интернет.

GSM-шлюз – устройство, позволяющее переводить телефонный трафик из сетей традиционной телефонии напрямую в сети сотовой связи стандарта GSM (и обратно). GSM-шлюз по своей сути представляет собой обычный мобильный телефон с собственной SIM-картой. Пример: GoIP.

SIM-банк – устройство, позволяющее подключить несколько SIM-карт. При этом связь с GSM-шлюзом осуществляется по сети, что позволяет разместить эти устройства на большом географическом удалении друг от друга.

Виртуальная АТС (англ. Hosted PBX) – это услуга обеспечения телефонной связи для компаний, которая заменяет физическую офисную мини-АТС и даже кол-центр. Пример: Astersisk.

IP-телефония (англ. IP telephony) – телефонная связь по протоколу IP. IP-телефония использует более общую технологию **VoIP** (англ. Voice over Internet Protocol) для организации двустороннего общения. Технология VoIP в общем случае подразумевает все варианты передачи голоса через IP, в том числе не имеющие никакого отношения к телефонии и общению людей.

Протокол установления сеанса (англ. Session initiation protocol (SIP) – протокол сеансового установления связи, обеспечивающий передачу голоса, видео, сообщений систем мгновенного обмена сообщений и произвольной нагрузки. Для сигнализации обычно использует порт 5060 UDP.

Софтфон (англ. Softphone) – класс ПО, предназначенный для совершения телефонных (голосовых) звонков или видеозвонков через Интернет. Пример: MicroSIP.

MDM (управление мобильными устройствами, англ. Mobile device management) – набор сервисов и технологий, обеспечивающих контроль и защиту мобильных устройств, используемых организацией и ее сотрудниками.

Джейлбрейк («рут», англ. Jailbreak, Root) – операция, позволяющая обойти ограничения, установленные производителем мобильного устройства, в целях получения доступа к устройству на более низком уровне (например, хранимым данным).

ADB (англ. Android debug bridge) – утилита, позволяющая взаимодействовать с мобильным устройством под управлением ОС Android. Используется разработчиками для управления и отладки мобильных приложений.

DFU (англ. Device firmware upgrade) – режим работы мобильного устройства, используемый для обновления прошивки.

BFU (англ. Before first unlock) – состояние мобильного устройства после включения или перезагрузки до того, как оно было разблокировано.

ГЛАВА 3. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ – SOFTWARE

Алгоритм (англ. Algorithm) – конечное упорядоченное множество точно определенных правил для решения конкретной задачи [1].

Программа (компьютерная) (сленг «прога», англ. Computer program) – комбинация компьютерных инструкций и данных, позволяющая аппаратному обеспечению вычислительной системы выполнять вычисления или функции управления [4].

Дистрибутив (сленг «дистр», англ. Distributive) – форма распространения ПО [1].

Примечание. Как правило, содержит набор файлов, составляющих программу, инструкции по установке, зависимости от других программ и автоматизированный установщик.

Инсталляция (сленг «сетап», англ. Install, Setup) – установка ПО в вычислительной системе с дистрибутива [1].

Примечание. Обратной операцией является деинсталляция (англ. Uninstall) – удаление установленного ПО.

Портирование (англ. Porting) – процесс адаптации ПО для запуска в другой программной среде.

Системная программа (программное обеспечение) (англ. System program (System software) – программа (ПО), предназначенная для поддержания работоспособности системы обработки информации или повышения эффективности ее использования в процессе выполнения прикладных программ [14].

Прошивка (микропрограмма, сленг «фирмварь», англ. Firmware) – программа, записанная на микросхеме постоянного

запоминающего устройства и управляющая работой аппаратного средства [1].

Прикладная программа (приложение, сленг «апликуха», англ. Application program) – программа, предназначенная для решения задачи или класса задач в определенной области применения системы обработки информации [14].

Утилита (сленг «тулза» (англ. Tool), англ. Utility) – прикладное ПО, предназначенное для выполнения вспомогательной (узкоспециализированной) задачи.

Фреймворк (англ. Software framework) – вид программной платформы, представляющей собой архитектурный «каркас», реализующий базовую функциональность, который, в свою очередь, может быть дополнен новой функциональностью.

SCADA (англ. Supervisory control and data acquisition – диспетчерское управление и сбор данных) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. Может являться частью АСУ ТП.

Операционная система – Operating system

Операционная система (ОС, англ. Operating system (OS) – программная надстройка, обеспечивающая пользовательский интерфейс, управление оборудованием и распределение аппаратных ресурсов. Согласно ГОСТ 15971–90 «Системы обработки информации. Термины и определения», под ОС понимается совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг. Примеры ОС: MS-DOS, Microsoft Windows, Apple MacOS (ранее OS X), Apple iOS, Android, Linux (распростра-

ненные дистрибутивы Linux: Debian, Ubuntu, CentOS, ArchLinux), FreeBSD.

Зависание (англ. Hang, Freeze) – явление в вычислительной технике, при котором устройство или программа перестает реагировать на действия пользователя либо на управляющие сигналы со стороны ОС, например в результате ожидания завершения операции чтения диска.

Экран смерти (синий экран смерти, сленг «бсод», англ. Blue screen of death (BSOD) – сообщение, которое появляется при возникновении критичной ошибки в ОС, работу которой невозможно продолжить без перезагрузки системы, что ведет к потере данных.

Драйвер, модуль ядра (англ. Driver, Kernel module) – программный компонент ОС, позволяющий расширять функциональные возможности ОС, например управлять внешним устройством либо осуществлять доступ к объектам ОС, которые недоступны обычным пользовательским программам (фильтрация и модификация сетевого трафика, перехват операций чтения-записи диска).

Снимок экрана (сленг «скриншот», «скрин», англ. Screenshot) – изображение экрана в определенный момент времени, которое сохранено в виде файла или скопировано в буфер обмена.

Сервис (служба, деймон, англ. Service, Daemon) – специальное ПО (процесс), работающее в фоновом режиме («на заднем плане», не отображая никаких окон) и выполняющее определенную задачу. Может взаимодействовать с клиентами сервиса по сети, представляя собой «сетевой сервис». Пример: ПО, реализующее веб-сервер, принимает HTTP-запросы от клиентов, а в ответ отдает содержимое веб-страниц.

Контроль учетных записей пользователей (англ. User account control, UAC) – компонент ОС Microsoft Windows, запрашивающий подтверждение действий, требующих права ад-

министратора, в целях защиты от использования административных функций без ведома пользователя.

Реестр Windows (реестр, системный реестр Windows, англ. Windows Registry) – иерархически построенная база данных в ОС семейства Microsoft Windows, содержащая настройки ОС и приложений.

Куст реестра (ветвь реестра, англ. Hive) – группа разделов, подразделов и параметров реестра с набором вспомогательных файлов, содержащих резервные копии этих данных [1].

Раздел реестра (ключ реестра, англ. Registry key) – заголовок реестра, обеспечивающий структуру для хранения конфигурационных значений и другой информации, которая необходима ОС Windows и установленным в ней приложениям [1].

Развертывание ПО (сленг «деплой», англ. Software deployment) – процесс приведения ПО к готовности к использованию.

DevOps (сленг «девопс», англ. Development, Operations) – набор практик, объединяющий процесс разработки ПО и его обслуживания.

CI/CD (непрерывная интеграция (англ. continuous integration) / непрерывное развертывание (англ. continuous delivery/deployment) – процесс, объединяющий разработку, сборку, тестирование и развертывание приложения.

Интегрированная среда разработки (англ. Integrated development environment, IDE) – система программных средств, используемая программистами для разработки ПО. Включает в себя редактор кода, отладчик, компилятор и т. д. Примеры: Visual Studio, VSCode, IntelliJ IDEA.

Переменная окружения (переменная среды, англ. Environment variable (ENV) – текстовая переменная ОС, хранящая какую-либо информацию, например данные о настройках системы. Используется для передачи различных параметров прикладным программам.

Пользовательский интерфейс – User interface

Графический интерфейс пользователя (сленг «гуи»/«гуй», англ. Graphical user interface (GUI) – вид пользовательского интерфейса, позволяющий взаимодействовать с системой посредством элементов интерфейса (кнопки, окна, значки и т. д.) в виде графических изображений.

Командная строка (англ. Command line interface (CLI); командная оболочка, сленг «шелл», англ. Shell; консоль, англ. Console; терминал, англ. Terminal) – способ взаимодействия (интерфейс) пользователя с ОС, принимающий от пользователя текстовые команды и предоставляющий вывод результатов указанных команд в текстовом виде.

Меню (сленг «менюшка», англ. Menu) – список параметров, из которого пользователь может выбрать параметр для выполнения требуемого действия [1].

Модальное окно (сленг «модалка») – окно пользовательского интерфейса, перекрывающее остальные окна и блокирующее доступ к ним, пока пользователь не выполнит действие, приводящее к его закрытию.

Панель задач (англ. Taskbar) – элемент интерфейса ОС, расположенный с края экрана, на котором отображаются запущенные программы.

Область уведомлений (сленг «трей», англ. System tray) – панель рядом с системными часами (обычно справа снизу), в которой расположены системные значки (регулятор громкости, управление беспроводными сетями и т. д.).

Разработка программного обеспечения – Software development

Язык программирования – формализованный язык, предназначенный для записи компьютерных программ. Принято разделять по принципу исполнения программ на компилируемые и интерпретируемые. В первом случае исходный код на

языке программирования преобразуется в машинный код. Во втором случае код программы исполняется при помощи интерпретатора. Пример: C++ (компилируемый), JavaScript (интерпретируемый).

Исходный код (сленг «исходник», «сорец», «сорцы», англ. Source code) – текст программы на каком-либо языке программирования, из которого можно получить исполняемый файл.

Скрипт (сценарий, англ. Script) – код программы на интерпретируемом языке программирования. Для разработки веб-приложений на клиентской части (в интернет-браузере) используются скрипты на языке программирования JavaScript. Распространенными скриптовыми языками общего назначения также являются Perl (сленг «перл»), PHP (сленг «пых», «пхп»), Python (сленг «питон», «пайтон»), Ruby (сленг «руби»), Lua, TCL (сленг «тикль»).

Компиляция – процесс преобразования кода на языке программирования в исполняемый (машинный или виртуальный) код. Выполняется с помощью специального ПО, называемого компилятором.

Интерпретатор (англ. Interpreter) – ПО, исполняющее код на интерпретируемом языке программирования (скрипт).

Исполняемый файл (сленг «экзешник», «бинарник», англ. Executable File) – файл программы, содержащий, в частности, машинный код и способный выполняться самостоятельно в ОС.

Примечание. Исполняемый файл может иметь пиктограмму («иконку»). В ОС семейства Microsoft Windows исполняемые файлы (в PE-формате) обычно имеют расширение «.exe», в то время как в ОС Linux исполняемые файлы (в формате ELF) обычно не имеют расширения.

Ассемблер (язык ассемблера, сленг «асм», англ. Assembly language) – низкоуровневый язык программирования, состоящий из инструкций для центрального процессора.

Спецификация требований ПО (англ. Software requirements specification, SRS) – комплексное описание ПО, которое требуется разработать.

Примечание. Аналогом является техническое задание (ТЗ) на разработку ПО.

Сборка (сленг «билд», англ. Build) – экземпляр собранного (скомпилированного) объекта, в частности исполняемого файла из исходных кодов.

Баг-трекер (англ. Bugtracker) – система отслеживания ошибок, используемая разработчиками ПО, позволяющая вести учет процесса разработки с помощью системы заявок (тикетов).

Тикет (англ. Ticket) – это заявка в системах отслеживания ошибок («баг-трекеров») для постановки задач и отслеживания их выполнения. У каждого тикета есть атрибуты, указывающие на приоритетность (низкая (Low), обычная (Normal), высокая (High), высочайшая (Highest) и важность задачи, а также указание ответственного за выполнение задачи пользователя. Список тикетов может быть представлен на специальной странице «Дашборд» (англ. Dashboard).

Динамическая библиотека (сленг «либа», «длл», англ. Dynamic library) – исполняемый код (машинный, предназначенный для прочтения вычислительным устройством), загружаемый в память процесса либо при его создании, либо по запросу уже работающего процесса (т. е. динамически). В ОС семейства Microsoft Windows представлены в виде файлов с расширением «.dll», в ОС Linux имеет расширение «.so».

API (сленг «апи», англ. Application programming interface) – программный интерфейс с определенным заранее набором ме-

тодов, позволяющих различным программным компонентам взаимодействовать друг с другом. Например, веб-сервис, предоставляющий API, при запросе определенного вида выдает данные в известном формате, пригодном для обработки сторонними программами.

Жизненный цикл ПО (англ. Systems development life cycle (SDLC) – период времени, который начинается с момента принятия решения о необходимости создания ПО, последующего его проектирования и заканчивается в момент прекращения его эксплуатации.

Обфускация (запутывание кода, англ. Obfuscation) – приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

Патч (сленг, «заплатка», англ. Patch) – исправление или дополнение ПО, устраняющее недостаток или ошибку.

Апгрейд (сленг, англ. Upgrade) – модернизация программного или аппаратного обеспечения.

Апдейт (сленг, англ. Update) – обновление (например, ПО).

Фикс (сленг, англ. Fix) – устранение ошибок (например, в программном коде).

Обновление безопасности (англ. Security update) – частный случай обновления, исправляющего только найденные уязвимости в ПО, но не добавляющего новый функционал.

Плагин (англ. Plugin), **Расширение** (сленг «экстеншн», англ. Extension), **Дополнение** (сленг «аддон», англ. Addon) – программный модуль, динамически (во время работы) подключаемый к основной программе и позволяющий расширять ее функциональные возможности.

Java (программная платформа) – комплекс ПО для разработки и исполнения программ, написанных на языке программирования Java.

Java-апплет – прикладная программа под программную платформу «Java», выполняемая в интернет-браузере.

Система контроля (управления) версий (англ. Version control) – система, предназначенная для совместной разработки ПО, в том числе организации репозитория (хранения) исходного кода. Пример систем контроля версий ПО: CVS, Subversion (SVN), Git.

Упаковщик (сленг «пакер», англ. Packer) – утилита, сжимающая исполняемые файлы в целях уменьшения их размеров. Примером распространенного упаковщика является UPX. Результатом работы упаковщика также является программа, но меньшего размера.

Псевдокод – язык описания алгоритмов, использующий ключевые слова языков программирования, но опускающий подробности и специфический синтаксис. Используется для упрощенного описания порядка действий.

Ревизия (англ. Revision) – применительно к системе контроля версий зафиксированное состояние хранилища исходного кода (после внесения изменений в исходный код), имеющее уникальный последовательный номер.

Хардкод (англ. Hard code) – заранее («жестко», статически) прописанные разработчиком в исходном коде значения параметров, позволяющие их использовать независимо от внешней среды, т. е. вместо получения этих значений из внешних источников (динамически), таких как пользовательский ввод, файлы конфигурации, база данных и т. д.

SDK (англ. Software development kit) – набор для разработки ПО под определенную программную платформу или систему, обычно содержащий утилиты, библиотеки, документацию и примеры кода. Набор для разработки ПО под программную платформу Java называется JDK (англ. Java development kit).

DDK (англ. Driver development kit) – набор утилит и библиотек для разработки драйверов под конкретную ОС.

Развертывание ПО (сленг «деплой», англ. Software deployment) – деятельность по приведению программной системы к использованию.

Обратная разработка (реверс-инжиниринг)

Реверс-инжиниринг – процесс восстановления алгоритма работы компьютерной программы или модуля без доступа к исходному коду на языке высокого уровня.

Реверс-инженер (сленг «реверсер») – специалист, исследующий алгоритм работы исполняемого кода без наличия исходного кода на языке программирования (так называемый методом реверс-инжиниринга или обратного инжиниринга).

Отладчик (сленг «дебаггер», англ. Debugger) – программа, позволяющая тестировать и анализировать алгоритм работы других программ.

Дизассемблер – программа, позволяющая получить из бинарного файла код на языке ассемблера.

Декомпиляция – процесс преобразования из исполняемого кода (машинного, предназначенного для прочтения вычислительным устройством) в псевдокод на языке программирования высокого уровня (предназначенного для восприятия человеком). Выполняется с помощью специального ПО, называемого декомпилятором.

Инжект (внедрение в процесс, англ. Inject) – внедрение стороннего кода в адресное пространство целевого процесса для получения контроля над последним. Например, внедрение в контекст интернет-браузера позволяет модифицировать поведение веб-страниц, отображаемых пользователю.

Антиотладка (англ. Anti-debugging) – методы и приемы, используемые при написании программного кода, препятствующие запуску исполняемого кода в отладочной среде, что усложняет анализ его алгоритма. Может включать в себя методы против эмуляции антивирусным ПО (антиэмуляция).

Протектор (англ. Protector) – утилита, защищающая ПО от анализа алгоритма его работы и модификации путем обфускации, упаковки и шифрования исполняемого кода, использования антиотладочных методов и т. д. (см. Упаковщик, Криптор).

Уязвимости программного обеспечения, эксплуатация уязвимостей

Уязвимость (сленг «дыра», англ. Vulnerability) – слабость программного (программно-технического) средства или информационной системы в целом, которая может быть использована для реализации угроз безопасности информации [6].

Уязвимость нулевого дня (сленг «зиродей», англ. Zero-day/0-day) – уязвимость, которая становится известной до момента выпуска разработчиком ПО информационной системы мер защиты информации по ее устранению, исправлений ошибок или соответствующих обновлений [6].

Уязвимость первого дня (англ. 1-day) – уязвимость ПО, которая устранена разработчиком данного ПО.

Эксплоит (эксплуатировать, англ. Exploit) – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые для проведения атаки на вычислительную систему.

Эксплоит-пак (связка эксплоитов, сленг «связка», англ. ExploitPack, ExploitKit (EK) – набор эксплоитов сразу под несколько программ и их версий и (или) под разные уязвимости в них.

Трафик (траффик, сленг «траф», англ. Traffic) – применительно к массовой эксплуатации уязвимостей поток перенаправленных на эксплоит (или эксплоит-пак) посетителей (перенаправленных веб-браузеров). Измеряется в количестве переходов.

Полезная нагрузка (сленг «пейлоад», англ. Payload) – часть передаваемых данных, содержащая значимую для источ-

ника передачи информацию. В области эксплуатации уязвимостей роль полезной нагрузки может выполнять **«шелл-код»** (от англ. Shellcode) – последовательность машинных инструкций (машинного кода), выполняющих определенные действия.

Песочница (англ. Sandbox) – изолированная среда для исполняемых файлов. Одно из предназначений песочницы – использование для анализа поведения потенциально опасных объектов, в том числе ВПО.

Фаззинг (англ. Fuzzing) – метод поиска уязвимостей в ПО путем автоматизированной подачи на вход программы некорректных данных в целях вызова нестандартного поведения.

CVE (англ. Common vulnerabilities and exposures) – публичная база известных уязвимостей, учет которой ведется некоммерческой организацией MITRE. Каждой уязвимости присваивается уникальный идентификатор. Пример идентификатора: CVE-2016-6786 указывает на уязвимость в ОС Linux, опубликованную в 2016 г., с порядковым номером 6786.

Багбаунти (англ. Bug bounty) – программа финансового поощрения, предлагаемая веб-сайтами, разработчиками ПО или организациями за обнаружение уязвимостей в их продуктах.

ГЛАВА 4. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ – MALWARE

Вредоносные объекты – Malicious objects

Вредоносное программное обеспечение (ВПО) (сленг «зловред», «малвара/малварь», англ. Malware) – ПО, изначально разрабатываемое для уничтожения, блокирования, модификации и копирования информации, несанкционированной ее владельцем, или иного нарушения процессов обработки, хранения и передачи информации.

Потенциально опасное ПО (ПО двойного назначения, англ. Riskware, Hacktool) – легальное ПО, которое может быть использовано злоумышленником в своих целях. Хотя данное ПО заведомо не создано для этих целей, в силу своих функциональных возможностей позволяет нарушить конфиденциальность, доступность или целостность данных. Примерами потенциально опасного ПО являются программы для удаленного доступа, восстановления паролей или ПО, используемые для анализа защищенности.

Антивирусное ПО (антивирус (АВ), сленг «авер», англ. Antivirus software) – средство защиты от потенциально опасных объектов, в частности ВПО.

Сэмпл (сленг, англ. Sample) – образец вредоносного ПО.

Детектирование (сленг «детект», англ. Detect) – процесс обнаружения антивирусным ПО потенциально опасных объектов или действий.

Сигнатура (вредоносного объекта) – характерные признаки вредоносного ПО, по которым средства защиты их детектируют (обнаруживают).

Проактивная защита (сленг «проактивка», англ. Proactive cyber defense) – совокупность технологий и методов, используемых в антивирусном ПО, позволяющая детектировать (обнаруживать) неизвестное вредоносное ПО. Проактивная защита

использует такие методы, как эвристический анализ, эмуляцию кода, анализ поведения (реагирует на определенную последовательность действий вредоносного ПО), песочницу (англ. Sandbox) и др.

Эвристический анализ (эвристика, англ. Heuristic) – применительно к антивирусному ПО метод поиска неизвестных ранее вредоносных объектов, для которых отсутствуют сигнатуры.

Бот (англ. Bot) – ПО, позволяющее осуществлять удаленный контроль над ПК, в частности за счет выполнения команд, полученных от владельца ботнета. Бот может быть установлен на ПК как с санкции владельца ПК, так и без его ведома (несанкционированно). Также под «ботом» понимают ПК, контролируемый ботом (программой).

Ботнет (бот-сеть, англ. Botnet) – совокупность (сеть) сетевых узлов, контролируемых ботами. Данная сеть может быть как централизованной, т. е. состоящей из клиентских (бот) и серверной (командный центр) частей ПО, так и децентрализованной (одноранговой, где все узлы сети равноправны).

Обход детектирования – процесс сокрытия компьютерной программой части своего функционала с целью не быть обнаруженной антивирусными средствами.

Командный центр (CC, C2 (англ. Command center), сервер управления) – серверная часть программного комплекса, включающая «панель администрирования» (сленг «админка», «панелька»), предназначенная для управления ботнетом.

Стаб (англ. Stub) – часть самостоятельного кода, выполняющего определенную функцию. Применительно к упаковщикам (криптерам) – часть кода, отвечающая за распаковку (расшифровку) запакованного (зашифрованного) тела программы.

FUD (сленг «фуд», англ. Full undetectable) – обозначение (вредоносного) объекта, который не детектируется распространенным антивирусным ПО.

Примечание. Для проверки на детектирование всевозможным антивирусным ПО могут использоваться специализированные сервисы как официально взаимодействующие с антивирусными компаниями – virustotal.com, так и гарантирующие нераспространение третьим лицам загружаемых объектов (сэмплы) – scan4you, viruscheckmate, avcheck.

Веб-инжект (англ. Web-inject) – внедрение стороннего кода в целевую веб-страницу в контексте веб-браузера, которое позволяет менять поведение веб-страницы. Например, веб-инжект может быть использован для подмены платежных реквизитов в интернет-банке.

Криптор (англ. Cryptor) – программа, модифицирующая исполняемый файл путем шифрования его секции кода, может применяться в области разработки ВПО в целях усложнения анализа алгоритма и сигнатурного детектирования средствами защиты.

Морфер (англ. Morpher) – ПО, осуществляющее преобразование (морфинг, «морф») программного кода с сохранением алгоритма его работы, что применяется для обхода сигнатурного детектирования системами защиты.

Обратное подключение (реверс-подключение, сленг «бекконнект», «БК», «бек», англ. Backconnect (bc) – метод установления сетевого подключения, позволяющий обойти ограничения на сетевом уровне, в частности трансляцию сетевых адресов (NAT), при которой невозможно инициировать подключение с сетевым узлом в локальной сети из глобальной сети (через Интернет).

Примечание. Метод используется ВПО для получения удаленного доступа к инфицированному ПК за счет того, что последний сам инициирует соединение с удаленным сервером.

Загрузка Drive-by (англ. Drive-by download) – метод загрузки вредоносного ПО посетителю веб-сайта, производимый незаметно для него (посредством эксплоита) и не требующий каких-либо дополнительных действий.

Синкхол (сленг «воронка», англ. Sinkhole) – сервер (например, DNS-сервер), предоставляющий ложные данные о доменном имени, позволяющий атакующему перенаправить запросы на другой адрес назначения. Традиционно используется исследователями ВПО для маскирования под сервер управления в целях изучения ботнетов.

Скрытая загрузка (англ. Drive-by attack) – метод скрытой загрузки ВПО, не требующий каких-либо дополнительных действий от пользователя, при которой пользователь заходит на скомпрометированный веб-сайт.

Watering hole – стратегия целевых атак, при которой ВПО размещается на веб-сайтах, посещаемых потенциальными жертвами.

Классификация вредоносных объектов – Malware classification

Вирус (англ. Computer virus) – вредоносное ПО, которое без ведома пользователя саморазмножается на вычислительном устройстве (компьютере), при этом каждая последующая копия также обладает способностью к саморазмножению. В отличие от червей, вирусы не используют сетевые сервисы для своего распространения и проникновения на другие компьютеры. Некорректно называть все вредоносные объекты вирусами, так как вирусами является узкий класс ВПО.

Червь (англ. Worm) – вредоносное ПО, которое без ведома пользователя саморазмножается в вычислительных сетях, при этом каждая последующая копия также обладает способностью к саморазмножению.

Троянская программа (сленг «троян», «троянец», «троянский конь», англ. Trojan Horse) – класс вредоносных программ, не способных к самовоспроизведению и осуществляющих действия на вычислительном устройстве (ПК), не санкционированные его пользователем. Троянские программы можно классифицировать в зависимости от поведения, например: программа-шпион (Trojan-Spy), программа-банкер (Trojan-Banker), программа-шифровальщик (Trojan-Ransom), программа для скрытого удаленного управления (Trojan-Backdoor), программа-загрузчик (Trojan-Downloader, Trojan-Dropper) и т. д.

Банкер (банковский троян, англ. Banker) – вид троянской программы, осуществляющей кражу пользовательской информации, относящейся к банковским счетам, системам электронных денег и платежным картам.

Бекдор, бэкдор (англ. Backdoor) – программная закладка, позволяющая злоумышленнику получить несанкционированный доступ к системе, в которую она была внедрена.

Шпионское ПО (англ. Spyware) – тип вредоносного ПО, которое при установке перехватывает или получает частичный контроль над компьютером пользователя без согласия пользователя [16].

Кейлоггер, Клавиатурный шпион (англ. Keylogger) – ПО либо его часть, которая перехватывает последовательность нажатых клавиш на клавиатуре пользователем ПК.

Дроппер (англ. Dropper) – класс ПО, предназначенных для скрытой установки программ, содержащихся в теле дроппера, на вычислительное устройство (компьютер), в том числе без подтверждения пользователя.

Руткит (англ. Rootkit) – ПО, предназначенное для сокрытия объектов и активности, таких как сетевые подключения, запущенные процессы, файлы и т. д.

Буткит (англ. Bootkit) – вредоносное ПО, которое загружается до ОС, способное контролировать все этапы ее запуска и

изменять системный код. Буткит загружается из главной загрузочной записи (см. MBR) или загрузочного сектора.

Adware (сленг «адвара») – рекламное ПО, предназначенное для показа рекламных сообщений (баннеров), перенаправления браузера на рекламные веб-страницы, сбора данных маркетингового характера.

Программы-вымогатели (англ. Ransomware) – вредоносное ПО, блокирующее доступ пользователя к вычислительному устройству (ПК) или его данным: **блокировщики** (англ. Blocker, WinLocker) – путем их модификации, **шифровальщики** (криптеры, англ. Crypter) – в целях получения выкупа за восстановление доступа.

Эксплоит (англ. Exploit) – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые для проведения атаки на вычислительную систему.

Лоадер, **Загрузчик** (сленг «лодырь», англ. Loader, downloader) – разновидность вредоносных программ, предназначенная для скрытой загрузки из сети стороннего ПО (как правило, ВПО) и его последующего запуска.

Примечание. Через бота (лоадера или трояна-лоадера) может осуществляться загрузка на исполнение стороннего исполняемого кода в виде отдельного модуля, исполняемого файла или другой нагрузки.

RAT (англ. Remote administration/access tool/trojan) – название для ПО, предоставляющего удаленный доступ к вычислительному устройству (в том числе несанкционированный владельцем устройства), на котором оно запущено.

Кликер (англ. Clicker) – ПО, которое имитирует действия пользователя путем программного «нажатия» клавиш клавиатуры, движений и кликов мышью.

ГЛАВА 5. СЕТЕВЫЕ ТЕХНОЛОГИИ – NETWORKING

Вычислительная сеть – Computer network

Сетевой узел (узел вычислительной сети, хост, англ. Network host, Network node) – вычислительное устройство (сервер, рабочая станция, сетевое оборудование и т. д.), соединенное с другим устройством через вычислительную сеть (для обмена данными).

Примечание. Также включает в себя «Интернет вещей»: тостеры, холодильники, чайники, веб-камеры, «умный дом», имеющие доступ в Интернет. Сетевой узел обладает сетевым адресом.

Вычислительная сеть (компьютерная сеть, англ. Computer network) – система, обеспечивающая обмен данными между вычислительными устройствами (серверы, ПК, сетевое оборудование) – узлами сети (сетевыми узлами). Согласно ГОСТ 24402–88 «Телеобработка данных и вычислительные сети. Термины и определения» под вычислительной сетью понимается взаимосвязанная совокупность территориально рассредоточенных систем обработки данных, средств и (или) систем связи и передачи данных, обеспечивающая пользователям дистанционный доступ к ее ресурсам и коллективное использование этих ресурсов.

Оверлейная сеть (англ. Overlay network) – сеть, построенная «поверх» другой сети.

Одноранговая сеть (пиринговая сеть, P2P, англ. Peer-to-peer) – децентрализованная оверлейная сеть, в которой все участники сети («пиры», англ. Peer) равноправны.

Интернет (сленг «инет», «нет», «сеть», англ. Internet) – глобальная сеть, объединяющая вычислительные сети, исполь-

зующие набор протоколов (стек протоколов), именуемый TCP/IP.

Интранет (корпоративная сеть, англ. Intranet) – частная вычислительная сеть, используемая внутри конкретной организации (компании).

Автономная система (АС, англ. Autonomous System (AS) – группа IP-сетей, принадлежащих одному или нескольким операторам и имеющих общую политику маршрутизации. Каждая АС имеет свой уникальный номер, используемый для маршрутизации по протоколу BGP. Например, IP-адрес 87.250.250.242 принадлежит автономной системе AS13238, оператором которой является Yandex LLC.

IP («ай-пи», англ. Internet protocol) – основной сетевой протокол, используемый в Интернете.

IP-адрес (сленг «ип», «айпишник», англ. Internet protocol address) – сетевой адрес, уникальный в масштабах текущей используемой сети (см. Локальный адрес), однозначно отличающий сетевые устройства друг от друга.

Примечание. В распространенной четвертой версии протокола (IPv4) IP-адрес обычно представляется в виде четырех чисел (4 байт или 32 бит) от 0 до 255, называемых октетами и разделенных точкой. В новой (шестой) версии протокола IP-адрес имеет длину 16 байт (128 бит) и разделяется двоеточием. Пример IPv4-адреса – 74.125.131.102, IPv6-адреса – fe80::fab1:56ff:fed9:689.

Статичный адрес (статический адрес, постоянный адрес, англ. Static address) – сетевой адрес, который назначается в настройках сетевого устройства вручную либо выдается автоматически, но закреплен за данным устройством и не может быть присвоен другому устройству.

Динамический адрес (англ. Dynamic address) – сетевой адрес, автоматически назначаемый сетевому устройству на определенный период времени. Для получения сетевых настроек наиболее распространен протокол DHCP, использующий DHCP-сервер для распределения адресов. В качестве альтернативы могут быть использованы технологии Zeroconf (в частности, APIPA), не требующие отдельного сервера для распределения адресов, – сетевые узлы самостоятельно выбирают адрес из сети 169.254.0.0/16.

Локальный адрес (внутренний, частный, «серый», англ. Local address) – IP-адрес из определенного диапазона адресов, выделенного под локальные сети и не используемый в глобальной сети (Интернете). Локальные адреса принадлежат следующим основным диапазонам: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255.

Геолокация (англ. Geolocation) – определение географического местоположения вычислительного устройства либо само местоположение. Определение местоположения может производиться по IP-адресу (например, по базе данных GeoIP), MAC-адресу, с помощью GPS-приемника или иным способом.

Локальная сеть (локальная вычислительная сеть (ЛВС), сленг «локалка», англ. Local area network (LAN) – это группа компьютеров и (или) других устройств, совместно использующих единые каналы связи, часто расположенных в пределах одного или нескольких зданий [16].

MAC-адрес («мак-адрес», англ. Media access control) – уникальный идентификатор (аппаратный адрес), представленный в виде 12 шестнадцатеричных цифр (6 байт), присваиваемый для сетевого оборудования производителем (в частности, сетевая карта (плата расширения). При этом первые три байта указывают на производителя устройства. Пример: «70:3e:ac:31:71:5e», где «703eac» – производитель Apple, Inc. Стоит учитывать, что MAC-адрес устройства может быть подменен.

Доменное имя (англ. Domain name) – идентификатор, состоящий из букв, чисел и точек, уникальным образом определяющий имя веб-ресурса в системе адресации DNS.

Регистратор (доменных имен) (англ. Domain name registrar) – организация, уполномоченная регистрировать новые доменные имена.

Делегирование (доменного имени) – процесс передачи управления частью доменной зоны другому лицу.

Обратный DNS-запрос («обратная зона», англ. Reverse DNS lookup) – доменная зона, предназначенная для определения доменного имени по IP-адресу.

Примечание. Основное предназначение сервиса DNS – преобразование из доменного имени в IP-адрес.

DNS-сервер (англ. Name server) – система распределения доменных имен между веб-ресурсами, обеспечивающая привязку IP-адреса и доменного имени, в том числе преобразование их друг в друга.

TLD (англ. Top level domain) – домен верхнего (первого) уровня. Пример: .ru, .com, .net.

Сетевой интерфейс – точка взаимодействия с сетью, обычно выполненная в виде устройства (сетевой карты). Сетевой интерфейс характеризуется MAC- (аппаратный) и IP- (сетевой) адресами.

Сетевой трафик (англ. Network traffic) – объем данных, передаваемый по вычислительной сети в определенный момент времени. Сетевые данные в основном передаются в виде блоков данных определенного формата – **сетевых пакетов** (англ. Network packet). Трафик, проходящий через сетевой интерфейс, для последующего его анализа может быть записан (захвачен) в файл («дамп трафика»). Распространенным форматом файла является формат PCAP, воспринимаемый такими сетевыми

анализаторами (сленг «сниффер», англ. Sniffer), как tcpdump и Wireshark.

Сетевой порт (англ. Port) – логические (виртуальные) точки подключения, связанные с определенным коммуникационным протоколом для обеспечения межсетевого обмена [16].

Примечание. Сетевой порт может быть в статусе «слушается» (англ. Listening), если он ожидает подключения.

Стандартный порт (англ. Well-known port) – порт, используемый определенным сетевым сервисом по умолчанию. Например, браузер по умолчанию подключается на 80 TCP-порт, являющийся стандартным для протокола http. Примеры других стандартных портов: HTTPS – 443/tcp, FTP – 21/tcp, DNS – 53/udp, SSH – 22/tcp.

Демилитаризованная зона (ДМЗ, англ. demilitarized zone (DMZ) – физическая или логическая подсеть, которая обеспечивает дополнительный уровень защиты для внутренней частной сети организации. ДМЗ создает дополнительный уровень защиты сети между сетью Интернет и внутренней сетью организации, чтобы внешние стороны могли подключаться напрямую только к устройствам в DMZ, а не ко всей внутренней сети [16].

Трансляция сетевых адресов (сленг «нат», англ. Network address translation (NAT) – механизм преобразования IP-адресов, позволяющий нескольким локальным сетевым узлам использовать один публичный (внешний, «выходной», «белый») адрес для доступа в глобальную сеть. Таким образом, сетевой узел, расположенный «за натом», не доступен из глобальной сети напрямую по своему локальному IP-адресу.

Виртуальная локальная сеть (сленг «влан», «вилан», англ. virtual LAN, Virtual Local Area Network (VLAN) – логиче-

ская локальная сеть, которая выходит за пределы одной традиционной физической локальной сети [16].

IP-телефония (англ. IP telephony, VoIP, Voice over IP) – общее название для технологий, обеспечивающих передачу голоса в сетях по протоколу IP.

Электронная почта (сленг «мыло», «мейл», англ. E-mail) – корреспонденция в виде сообщений, передаваемая между пользователями через вычислительную сеть [1].

Domain Fronting – метод маскировки реального адреса сетевого ресурса, к которому устанавливается соединение, путем манипулирования запросами к сети доставки контента (CDN), что позволяет обойти ограничения на сетевом уровне.

Сеть доставки контента (англ. Content delivery / distribution network (CDN) – географически распределенная сетевая инфраструктура, позволяющая оптимизировать доставку содержимого (контента) конечным пользователям в Интернете. Пример: Cloudflare.

Облачные вычисления (облако, англ. Cloud computing) – вариант предоставления услуг, при котором пользователь получает необходимые вычислительные ресурсы по запросу. Пример: Amazon AWS.

Kerberos (krb) – сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причем в протоколе учтен тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Использует аутентификационные билеты (сленг «тикет», (TGT), англ. ticket granting ticket). Злоумышленниками для закрепления в системе может использоваться так называемый **Golden ticket**.

Фронтенд (сленг «фронт», англ. Front-end) – клиентская часть программно-аппаратной части сервиса. Применительно

к веб-сайтам (веб-приложениям) часть программного кода, выполняемая на стороне пользователя в браузере. Отвечает за пользовательский интерфейс и взаимодействие с сервером (сленг «бек», англ. Back-end) посредством API (например, REST, JSON-RPC, gRPC и т. д.). Для разработки клиентской части сложных веб-приложений применяются «реактивные» фреймворки, такие как React, Vue.JS, Angular.

Netflow (сленг «нетфлоу») – сетевой протокол, используемый для учета сетевого трафика. Предоставляет сетевую статистику и информацию о подключениях. Развитием протокола Netflow является стандарт IPFIX (Internet protocol flow information export).

Технология Push (англ. Push technology, server push) – вид сетевого взаимодействия, при котором сведения передаются от сервера (поставщика) пользователю в виде уведомлений.

KVM-переключатель (аббр. англ. keyboard, video, mouse – клавиатура, видео, мышь) – устройство, предназначенное для коммутации одного комплекта устройств ввода-вывода между несколькими компьютерами. Последнее поколение KVM-переключателей может передавать видеосигнал и ввод с мыши/клавиатуры по сети (IP-KVM) и использоваться для удаленного доступа.

IPMI (англ. Intelligent platform management interface) – это интерфейс для удаленного мониторинга и управления физическим состоянием сервера.

Сервер приложений (англ. Application server) – это специальное ПО, снабжающее среду выполнения для прикладных программ.

Даркнет (англ. Darknet) – оверлейная сеть в Интернете, для доступа к которой необходимы специальное ПО, конфигурация или разрешение (авторизация). См. TOR.

Веб (Всемирная паутина, англ. World wide web (WWW) – веб-ресурсы, доступные в Интернете.

Глубинный веб (Глубокая сеть, англ. Deep web) – веб-ресурсы в Интернете, недоступные для индексации поисковыми системами.

Привилегированный пользователь (суперпользователь, «админ», сленг «рут» (от англ. root), англ. Privileged user) – пользователь, обладающий расширенными правами доступа к системе.

Сетевое оборудование – Network devices

Сетевое оборудование (англ. Network devices) – устройства, обеспечивающие работу вычислительной сети. Примеры: сетевой адаптер (сетевая карта), маршрутизатор (роутер), коммутатор (свитч).

Сетевой адаптер (сетевая карта/плата, сленг «сетевуха», англ. Network interface controller/card (NIC) – оборудование, посредством которого вычислительное устройство подключается к вычислительной сети (см. Сетевой интерфейс). Как любое другое сетевое устройство, сетевой адаптер имеет свой уникальный MAC-адрес.

Модем (сленг «мопед», «свисток» (применительно к USB-модемам), англ. Modem) – устройство, позволяющее передавать цифровые данные по аналоговым каналам передачи данных, в частности через сети операторов мобильной связи.

Маршрутизатор (сленг «роутер», англ. Router) – аппаратное или ПО, которое соединяет две или более сетей [16].

Коммутатор (свитч, англ. Switch) – устройство, позволяющее объединить несколько сетевых устройств в единую вычислительную сеть.

Межсетевой экран (МЭ/МСЭ) (брандмауэр, фаервол, сленг «фаер», англ. Firewall) – аппаратная и (или) программная технология, которая защищает сетевые ресурсы от несанкционированного доступа. Межсетевой экран разрешает или запре-

щает трафик между сетями с различными уровнями безопасности на основе набора правил и других критериев [16].

Зеркалирование портов (сленг «спан», англ. Mirroring, Switched port analyzer (SPAN) – функциональность коммутатора, позволяющая дублировать сетевой трафик одного сетевого порта на другой.

DPI (англ. Deep packet inspection) – вид обработки передаваемых по каналу связи данных, позволяющий проверять и фильтровать сетевые пакеты по их содержимому.

Беспроводные сети – Wireless network

Беспроводные сети (англ. Wireless network) – вычислительная сеть, основанная на беспроводном принципе работы, например использовании радиоволн в качестве носителя информации.

Примечание. Наиболее распространенной технологией создания беспроводных вычислительных сетей, использующих радиоволны, является Wi-Fi.

Беспроводная точка доступа (англ. Wireless access point (AP) – устройство, с помощью которого беспроводные коммуникационные устройства подключаются к беспроводной сети. Обычно беспроводная точка доступа подключается к проводной сети и может передавать данные между беспроводными и проводными устройствами в сети [16].

Bluetooth – протокол беспроводной связи, который использует технологию связи ближнего действия для передачи данных на короткие расстояния [16].

WEP (англ. Wired equivalent privacy) – слабый алгоритм шифрования, используемый для беспроводных сетей [16].

WPA, WPA2 (англ. Wi-Fi protected access) – протокол безопасности, созданный для защиты беспроводных сетей. WPA

является преемником протокола WEP. WPA2 – это новое поколение технологии WPA [16].

WPS (англ. Wi-Fi protected setup, Quick security setup(QSS) – стандарт создания защищенной домашней беспроводной сети, позволяющий упростить ее настройку. При этом в протоколе WPS была обнаружена уязвимость, с помощью которой злоумышленник может подключиться к беспроводной сети.

Сетевые туннели, средства анонимизации

Прокси-сервер, **Прокси** (англ. Proxy) – промежуточный сервер для трансляции запросов. Обычно под прокси понимается HTTP-прокси – прокси, транслирующий HTTP-запросы, однако могут использоваться другие протоколы, например Socks. Прокси называется «прозрачным» (англ. Transparent), если перенаправление осуществляется незаметно для конечного пользователя.

Виртуальная частная сеть (VPN) (сленг «впн», англ. Virtual private network) – общее название технологии организации защищенного (зашифрованного) сетевого соединения поверх другой сети (построение сетевого туннеля). Данная технология в том числе позволяет перенаправлять сетевой трафик через сторонний сетевой узел, тем самым скрывая первоначальный источник трафика.

Tor (сленг «луковый маршрутизатор», англ. Tor (The onion router) – открытое ПО, реализующее одноименную анонимную сеть. Соединение в сети Tor организуется через цепочку посредников (через «узлы» – Tor-ноды (англ. Tor node), каждый из которых имеет информацию только о предыдущем и о следующем «узле». На «выходном узле» (англ. Exit node) сетевой трафик полностью расшифровывается и может быть перехвачен.

Тор-браузер (англ. TOR browser) – браузер, основанный на браузере Mozilla Firefox, предназначенный для анонимной работы через TOR.

Сетевые ресурсы, коммуникация

Система мгновенного обмена сообщениями («мессенджер», англ. Instant messaging (IM) – сетевой сервис, позволяющий его пользователям обмениваться сообщениями в режиме реального времени. Примеры сервисов: Jabber (XMPP), ICQ, Skype.

Блог (англ. Blog) – вид веб-сайта, представляющего собой формат дневника, состоящего из публикуемых блогером (лицо, отвечающее за публикацию) записей (постов).

Вики (англ. Wiki) – вид веб-сайта, содержимое которого редактируется его пользователями. Примером является интернет-энциклопедия «Википедия» (англ. Wikipedia), статьи в которой может создавать и изменять любой желающий.

Спам (англ. Spam) – массовая рассылка сообщений (посредством электронной почты, систем мгновенного обмена сообщениями и т. д.) рекламного или иного характера без явного согласия на то получателя. Сообщения, рассылаемые таким образом, могут содержать вредоносные объекты.

Skype («скайп») – система, позволяющая осуществлять голосовые вызовы, обмениваться текстовыми сообщениями и файлами любых типов, используя сеть Интернет.

Jabber (Джаббер, англ. Extensible messaging and presence protocol (XMPP) – сервис мгновенного обмена сообщениями. Сервис является децентрализованным (не имеет единого общего сервера), что позволяет любому пользователю сети создать свой, независимый от других пользователей, Jabber-сервер.

BitTorrent (Торрент) – децентрализованный протокол для обмена файлами (см. Одноранговая сеть), при этом файлы хра-

нятся и раздаются с компьютеров участников. Информацию о «раздачах» предоставляет специальный сервер – торрент-трекер.

Веб-технологии – Web technologies

RFC (англ. Request for comments) – набор документов, описывающих технические и организационные аспекты сети Интернет, включая описание протоколов, процедур, программ и концепций. Так, документ RFC 2616 описывает протокол HTTP.

Браузер (интернет-браузер, веб-браузер, устар. «веб-обозреватель», англ. Web browser) – прикладное ПО, предназначенное для взаимодействия с интернет-ресурсами, в частности для просмотра веб-сайтов.

Веб-сайт (англ. Web site) – совокупность логически связанных между собой веб-страниц (документов), доступ к которым осуществляется через веб-браузер.

Веб-сервер (англ. Web server) – сетевой сервис для предоставления доступа к веб-сайту. При этом между веб-сервером и интернет-браузером пользователя происходит взаимодействие в виде запроса-ответа по протоколу HTTP (HTTPS).

Веб-приложение (англ. Web application) – приложение, доступ к которому обычно осуществляется через веб-браузер или веб-службы. Веб-приложения могут быть доступны в сети Интернет или в частной, внутренней сети [16].

URL (Единый идентификатор ресурса, сленг «урл», англ. Uniform resource locator) – единообразный способ записи адреса ресурса в вычислительной сети. Пример: «http://yandex.ru/index.html», «ftp://guest:pass123@10.211.0.13:2121/public/readme.txt».

HTML (сленг «хтмл», англ. Hypertext markup language) – язык разметки, используемый для создания веб-страниц и описывающий их структуру, содержание и способ отображения.

HTML-тег (англ. HTML tag) – элемент языка разметки HTML, описывающий такие компоненты веб-страницы, как па-

раграф, заголовок, таблица, изображение и т. п. Пример «блочного» тега «div»: Hello .

JavaScript (JS) – интерпретируемый (выполняемый напрямую из исходного кода) язык программирования, используемый как одна из базовых технологий создания веб-страниц.

User-Agent (UA, «юзер-агент») – один из заголовков (поле с данными) HTTP-запроса к веб-серверу, который указывает на ПО, используемое посетителем ресурса, в частности версию браузера и его плагинов. User-Agent, как и остальные заголовки HTTP-запроса, устанавливается на стороне клиента и поэтому может быть подделан. Пример значения User-Agent для браузера Google Chrome (использующий код из проекта WebKit), запущенного в ОС Linux: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.108 Safari/537.36, при этом отсылка к ПО Mozilla и Safari необходима для обратной совместимости.

Куки (сленг «кука», англ. Cookie) – небольшой объем данных (не больше 4 Кб), сохраняемый у пользователя в браузере. Куки могут содержать идентификатор сессии, идентификатор пользователя (UserID, UID) или другие данные (адрес электронной почты) для идентификации пользователя на веб-сайте.

Всплывающие окна (сленг «попапы», англ. pop-up) – элемент интерфейса в виде открываемого нового окна в интернет-браузере. Данное окно может быть использовано для перенаправления интернет-браузера на сторонний веб-ресурс. Современные браузеры блокируют всплывающие окна.

Редирект (англ. Redirect) – перенаправление интернет-браузера пользователя по определенному URL (адресу).

CAPTCHA («капча», англ. Completely automated public turing test to tell computers and humans apart) – один из вариантов теста Тьюринга, позволяющего определить, кем является пользователь – реальным человеком или программой (роботом), которая выдает себя за человека. Для прохождения теста пользо-

вателю дается трудновыполнимая для компьютерной программы задача: распознать искаженный текст на изображении, найти объекты на фотографии и т. д.

Поисковая оптимизация (сленг «сео», англ. Search engine optimization (SEO) – комплекс мероприятий, выполняемых специалистами по поисковой оптимизации – «сеошниками», целью которых являются повышение позиций сайта в результатах выдачи поисковых систем и увеличение количества посетителей. Отдельно стоит выделить так называемый черный сео (англ. Black SEO), при котором применяются методы, запрещенные правилами поисковых систем.

Adobe Flash (сленг «флеш») – программная технология для создания и исполнения интерактивных мультимедийных приложений (содержащих анимацию, видео и др.) (сленг «флешка»), доступных для просмотра с помощью ПО Adobe Flash Player, в том числе как элемент веб-сайта в контексте интернет-браузера (через плагин).

Фрейм (англ. Frame), «айфрейм» (англ. Iframe) – применительно к языку разметки HTML – HTML-тег, позволяющий вставить содержимое одной веб-страницы в контекст другой. Может применяться злоумышленниками для скрытого перенаправления на подконтрольный ему интернет-ресурс.

Сетевые сервисы и протоколы

Сетевой протокол – набор соглашений (правил), описывающих порядок взаимодействия с сетевыми сервисами или устройствами, в том числе для передачи данных. Пример: протоколы HTTP, FTP.

Защищенный протокол (англ. Secure protocol) – сетевой протокол, защищающий передаваемые данные путем их шифрования. Для генерации и обмена ключей шифрования часто используются протоколы с асимметричными алгоритмами шифрования. Для шифрования непосредственно передаваемых

данных часто используются симметричные алгоритмы шифрования.

Небезопасный протокол, служба или порт (англ. Insecure protocol/service/port) – протокол, служба или порт, которые создают проблемы безопасности вследствие недостатков механизмов защиты конфиденциальности и (или) целостности. К таким проблемам безопасности относятся службы, протоколы или порты, которые: передают учетные данные для аутентификации (например, пароль или парольные фразы) в виде незашифрованного текста по сети Интернет; позволяют легко воспользоваться уязвимостями, имеющимися в них по умолчанию или вследствие неправильной настройки. Примеры небезопасных сервисов, протоколов или портов включают, помимо прочих, FTP, Telnet, POP3, IMAP и SNMP версии 1 и 2 [16].

TCP (англ. Transmission control protocol) – один из базовых протоколов транспортного уровня стека протоколов TCP/IP, а также базовый язык коммуникации или протокол Интернета. См. IP [16].

UDP (англ. User datagram protocol) – один из базовых протоколов транспортного уровня. В отличие от TCP, в UDP нет процедуры установления соединения и UDP не гарантирует доставку пакетов («датаграмм»), поэтому протокол используется там, где важна скорость доставки данных, но не надежность (трансляция игр, сетевые игры и т. д.).

ICMP (англ. Internet control message protocol) – служебный протокол, используемый маршрутизаторами для отправки сообщений об ошибках (например, о том, что сетевой пакет не дошел до адресата), а также позволяет проверять доступность удаленного сетевого узла.

Ping (сленг «пинг») – утилита для проверки доступности удаленного сетевого узла (путем отправки по протоколу ICMP пакетов Echo request), позволяющая измерить среднее время прохождения сетевых пакетов (задержку). Также «пингом»

называют сам ICMP-запрос, процесс его отправки («пинговать») и время прохождения пакета.

DNS (система доменных имен, англ. Domain name system) – сетевой сервис, который отвечает за сопоставление (трансляцию, преобразование, разрешение (сленг «резолв», англ. Resolve) доменного имени в IP-адрес. Например, доменное имя ya.ru разрешается в IP-адрес как 87.250.250.242.

HTTP (англ. Hypertext transfer protocol – «протокол передачи гипертекста») – сетевой протокол передачи данных, используемый для взаимодействия с веб-сервером. Существует защищенное расширение протокола – HTTPS, реализующее шифрование данных и удостоверение подлинности веб-сервера.

FTP (сленг «ФТП», англ. File transfer protocol) – незащищенный сетевой протокол передачи файлов.

IMAP (англ. Internet message access protocol – сетевой протокол доступа к сообщениям) – сетевой протокол прикладного уровня, позволяющий почтовому клиенту получить доступ к электронным сообщениям на удаленном почтовом сервере [16].

POP3 (англ. Post office protocol v3) – протокол прикладного уровня, используемый почтовыми клиентами для получения электронных сообщений с удаленного сервера через подключение по протоколу TCP/IP [16].

IPSEC (англ. Internet protocol security) – стандарт для защиты соединений по протоколу IP на сетевом уровне посредством шифрования и (или) аутентификации всех IP-пакетов в коммуникационной сессии [16].

NTP (англ. Network time protocol) – сетевой протокол для синхронизации часов компьютерных систем, сетевых устройств и других системных компонентов [16].

SSH (англ. Secure shell, «безопасная оболочка») – набор протоколов, которые обеспечивают шифрование для сетевых служб, таких как удаленный вход в систему или удаленная передача файлов [16].

Telnet (англ. Telephone network protocol) – сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме – при помощи транспорта TCP). Учетные данные пользователя передаются в виде незашифрованного текста [16].

SSL (англ. Secure sockets layer) – общепринятый отраслевой стандарт шифрования канала связи между веб-браузером и веб-сервером, который обеспечивает конфиденциальность и достоверность данных, передаваемых по этому каналу [16].

TLS (англ. Transport layer security) – протокол, обеспечивающий защищенную передачу данных между узлами в Интернете. TLS является преемником протокола SSL [16].

WHOIS (сленг «хуиз») – сетевой сервис, предоставляющий информацию об IP-адресе или доменном имени.

Маска подсети (сетевая маска, англ. Subnet mask, netmask) – значение, указывающее, какая часть IP-адреса относится к адресу сети, а какая – к адресу самого узла в этой сети. Может задаваться в виде октетов (255.255.252.0) или в виде префикса (/24).

Локальный хост (англ. Localhost) – зарезервированное имя сетевого узла, которое указывает на текущий сетевой узел (IP-адрес 127.0.0.1).

Пиринговая сеть (англ. Peer-to-peer (P2P) – оверлейная вычислительная сеть, участники которой равны: каждый узел (сленг «пир», англ. Peer) является клиентом и одновременно выполняет функции сервера.

ГЛАВА 6. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – INFORMATION TECHNOLOGY

Базовые термины ИТ

Информационные технологии (ИТ) (англ. Information technology (IT) – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы их осуществления.

Информационная система (англ. Information system) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию [14].

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [15].

Искусственный интеллект (ИИ; англ. Artificial intelligence (AI) – технология создания умных программ и машин, которые могут решать творческие задачи и генерировать новую информацию на основе имеющейся. Фактически искусственный интеллект призван моделировать человеческую деятельность, которая считается интеллектуальной.

Машинное обучение (англ. Machine learning (ML) – класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение за счет применения решений множества сходных задач.

Глубокое обучение (глубинное обучение, англ. Deep learning) – совокупность методов машинного обучения, основанных на обучении представлениям, а не специализированным алгоритмам под конкретные задачи. Для глубокого обучения используется **(искусственная) нейронная сеть** (англ. (Artificial) neural networks, (A)NNs) – математическая мо-

дель, построенная по принципу сетей нервных клеток живого организма.

ИТ-инфраструктура – IT infrastructure

Системный администратор (сленг. «админ», «сисадмин», англ. System administrator, Sysadmin) – лицо, обладающее расширенными полномочиями и несущее ответственность за управление компьютерной системой или сетью [16].

Сервер (англ. Server) (ПО) – специализированное ПО, выполняющее сервисные (обслуживающие) функции по запросу клиента, предоставляя ему доступ к определенным ресурсам или услугам [7]. Также может быть **сервер** (сленг «сервак», англ. Server) (аппаратное обеспечение) – вычислительное устройство (компьютер или специальное оборудование), выполняющее определенную функцию (роль) и обеспечивающее работу специализированного ПО.

Интернет-провайдер (сленг «пров», англ. Internet service provider (ISP) – организация, предоставляющая доступ к Интернету. Выделяют провайдеров Интернета от магистральных (первичных), предоставляющих доступ преимущественно для других провайдеров, до провайдеров «последней мили» (домашний провайдер, сленг «выделенка»), предоставляющих доступ к сети конечным пользователям.

Дата-центр (англ. Data center), Центр (хранения и) обработки данных (ЦОД/ЦХОД) – помещение, предназначенное для размещения серверного и сетевого оборудования, обеспечивающее канал связи для оборудования.

Колокация (сленг «колокейшн», англ. Co-location, colo) – услуга, при которой провайдер (хостинг) размещает оборудование клиента (сервер) на своей территории.

Выделенный сервер (сленг «дедик», англ. Dedicated server) – сервер в виде реального аппаратного обеспечения (так

называемый bare metal), в отличие от виртуального сервера, предоставляемый клиенту хостинга целиком.

Виртуальный выделенный сервер (сленг «впс», англ. Virtual dedicated server (VDS) / Virtual private server (VPS) – виртуальный сервер, предоставляемый клиенту хостинга целиком, однако на гипервизоре могут располагаться виртуальные серверы разных клиентов.

Хостинг (англ. Hosting) – услуга по предоставлению вычислительных ресурсов. Так, веб-хостинг предоставляет клиентам ресурсы для размещения веб-сайта.

Виртуальный хостинг (сленг «шаред хостинг», англ. Shared hosting) – вид веб-хостинга, при котором веб-сайты разных клиентов располагаются на одном физическом сервере.

Абузоустойчивый хостинг (сленг «булитпруф хостинг», англ. Bulletproof hosting) – хостинг, устойчивый к поступающим от третьих лиц жалобам («абузам», англ. Abuse).

Конфигурация (сленг «конфиг», англ. Configuration) – набор настроек, который может храниться в базе данных, в конфигурационном файле или ином виде.

Резервная копия (сленг «бекап», англ. Backup) – копия данных, хранимая в целях восстановления в случае утери первичных данных. Резервная копия может быть как полной (копия всего объема данных), так и инкрементальной (копируются только внесенные изменения по сравнению с предыдущей копией).

Протокол (работы программы) (журнал событий, сленг «лог», англ. Event log, Journal) – файл с записями о событиях в хронологическом порядке [1].

Производственная версия (сленг «продакшн», «боевая версия», «продуктовая версия», англ. Production) – рабочая версия ПО или сервера, находящаяся в применении. Также могут выделяться версии, предназначенные для разработки (англ. Development), те-

стовые (англ. Testing, Staging) и резервные (сленг «стендбай», англ. Standby).

Домен Windows (англ. Windows domain) – объединенные службой каталогов Microsoft Active Directory (AD, сленг «АД») в одну сеть сетевые ресурсы (серверы, рабочие станции), управляемые централизованно администраторами домена с помощью контроллера домена (англ. Domain controller (DC), сленг «ДЦ»).

Учетная запись по умолчанию (англ. Default account) – учетная запись для входа, предварительно заданная в системе, приложении или устройстве и предназначенная для первоначального доступа к системе при ее начальном запуске. В процессе установки система может сгенерировать дополнительные учетные записи по умолчанию [16].

Пароль по умолчанию (англ. Default password) – пароль (как правило, связанный с учетной записью по умолчанию) к административным, пользовательским или служебным учетным записям, предварительно заданный в системе, приложении или устройстве. Учетные записи по умолчанию и пароли по умолчанию опубликованы, хорошо известны и поэтому легко угадываются [16].

Мониторинг (англ. Monitoring) – использование систем или процессов для постоянного наблюдения за компьютерами или сетевыми ресурсами в целях уведомления персонала в случае сбоя в работе, поступления сигнала тревоги или наступления иных предопределенных событий [16].

Удаленный доступ (англ. Remote access) – процесс управления сторонним вычислительным устройством через вычислительную сеть.

Системы удаленного доступа (управления) – ПО, позволяющее получить доступ к сетевому ресурсу (серверу, ПК) посредством сети (как локальной, так и глобальной). Примеры

протоколов удаленного управления: графические (GUI) – VNC (RFB), RDP, текстовые (командная строка) – SSH, Telnet.

Фронтенд (сленг «проброс», «прокладка», англ. Front-end, редиректор) – промежуточный сетевой узел (сервер), используемый в цепочке сетевых подключений. Может быть использован для затруднения процесса обнаружения сетевых ресурсов и их адресов (доменное имя, IP-адрес), располагаемых за фронтендом (промежуточные и оконечные сетевые узлы) – **бэкендов** (англ. Back-end).

База данных – Database

База данных (БД) (англ. Database (DB) – данные, представленные в виде организованной структуры в целях хранения и обработки, в частности для извлечения (поиска) данных. Простейшими примерами базы данных являются таблицы.

Система управления базами данных (СУБД) (англ. Database managment system (DBMS) – ПО, предназначенное для организации и ведения базы данных. Примеры клиент-серверных реляционных СУБД: MSSQL, Oracle, MySQL (сленг «мускул»), PostgreSQL (сленг «постгрес», psql), SQLite.

Реляционная БД – база данных, в которой данные представлены в виде именованных таблиц, состоящих из именованных столбцов (полей) и строк (записей). Взаимодействие производится посредством запросов на языке SQL (сленг «сиквел», англ. Structured query language) к базе данных. Пример запроса для получения данных: «SELECT id,name,password FROM users WHERE name=’John’;».

Репликация (англ. Replication) – процесс синхронизации (копирования) данных с резервным вычислительным устройством (сленг «стендбай», англ. Standby) в целях повышения надежности хранения данных. Распространенным методом репликации является схема, при которой источник данных назы-

вается ведущим (сленг «мастер», англ. Master), а резервное устройство – ведомым (сленг «слейв», англ. Slave).

Критическая информационная инфраструктура – Critical IT infrastructure

Автоматизированная система управления (АСУ) – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления оборудованием и процессами [3].

Безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении нее компьютерных атак [3].

Значимый объект критической информационной инфраструктуры – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры [3].

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов [3].

ГЛАВА 7. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) – INFORMATION SECURITY

Основные понятия ИБ

Информационная безопасность (англ. Information security) – защита информации для обеспечения конфиденциальности, целостности и доступности [16].

Безопасность информации (данных) (англ. Information (Data) security) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [2].

Целостность информации (англ. Integrity of information) – состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и (или) непреднамеренного воздействия на нее [12].

Конфиденциальность информации (англ. Confidentiality of information) – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2].

Кибер- (англ. Cyber-) – приставка, указывающая на принадлежность к цифровым технологиям. Пример: киберпреступление, кибербезопасность.

Кибербезопасность (англ. Cybersecurity) – область информационной безопасности, затрагивающая киберпространство.

Актив (англ. Asset) – все, что имеет ценность для организации. Различают следующие виды активов: информация; ПО; технические средства (например, компьютер); услуги и сервисы; люди и их квалификация, навыки и опыт; нематериальные активы (например, репутация и имидж) [13].

Доступ к информации – возможность получения информации и ее использования [1].

Несанкционированный доступ к информации (НСД, сленг «взлом», англ. Unauthorized access to information) – доступ к информации и ресурсам информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа к информации и ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по функциональному предназначению и техническим характеристикам [12].

Блокирование доступа к информации – прекращение или затруднение доступа законных пользователей к информации [14].

Инсайдер (англ. Insider) – сотрудник предприятия, который причиняет или планирует причинение ущерба активам организации или помогает в такой акции внешнему нарушителю [15].

Инцидент информационной безопасности (англ. Information security incident) – одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности [13].

Множественные уязвимости (англ. Multiple vulnerabilities) – две и более уязвимости, содержащиеся в компоненте ПО, сведения о которых опубликованы в общедоступных источниках информации [15].

Нарушитель безопасности информации (англ. Attacker (intruder, violator, troublemaker) – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах [14].

Событие информационной безопасности (англ. Information security event) – выявленное наступление состояния системы, сервисов или вычислительной сети, указывающее на возможное нарушение политики информационной безопасности,

на сбой или отсутствие необходимых мер защиты или на прежде неизвестную ситуацию, относящиеся к обеспечению безопасности [13].

Политика (англ. Policy) – совокупность установленных в организации правил, регламентирующих допустимое использование вычислительных ресурсов, практические меры по обеспечению безопасности и принципы разработки рабочих процедур [16].

Атака (компьютерная) – попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования [13].

Угроза (англ. Threat) – возможная причина нежелательного инцидента, которая может нанести ущерб (информационной) системе или всей организации [13].

Аутентификация (англ. Authentication) – процесс проверки подлинности в отношении человека, устройства или процесса. Аутентификация обычно выполняется посредством использования одного или нескольких аутентификационных факторов: обладание информацией (например, паролем или парольной фразой); обладание предметом (например, аппаратным токеном или смарт-картой); обладание параметрами (например, биометрическими) [16].

Авторизация (англ. Authorization) – предоставление определенному лицу или группе лиц прав на выполнение определенных действий, а также процесс подтверждения данных прав при попытке выполнения этих действий [1].

Учетная запись (аккаунт, сленг «акк», англ. Account) – совокупность данных пользователя, содержащих идентификатор пользователя в виде имени (логин, англ. Login) и пароля.

Учетные данные для аутентификации (сленг «креды», англ. Authentication credentials) – сочетание идентификатора пользователя или учетной записи и одного или нескольких

аутентификационных факторов, которые используются для проверки подлинности в отношении человека, устройства или процесса [16].

Пароль, парольная фраза (англ. Password, Passphrase) – строка символов, которая служит для аутентификации пользователя [16].

Привилегированный пользователь (англ. Privileged user) – любая учетная запись с правами доступа, превышающими базовые. Обычно такие учетные записи имеют больше прав, чем стандартная учетная запись. Однако объем прав разных привилегированных учетных записей может существенно различаться в зависимости от организации, должностных обязанностей или ролей и используемых технологий [16].

Одноразовый пароль (сленг «отп», англ. One time password (OTP) – пароль, который действителен только один раз и не может быть повторно использован. Используется для подтверждения конкретной операции. Частным случаем одноразового пароля является TAN-код (сленг «тан», англ. Transaction authentication number) – код подтверждения транз-акции, например получаемый в SMS-сообщении от банка, ввод которого в интернет-банке подтверждает выполнение финансовой операции.

Токен авторизации (аппаратный) (англ. Token) – устройство, используемое для идентификации и подтверждения подлинности (аутентификации) пользователя. Токен выполняется в виде смарт-карты, компактного USB-устройства, брелока, отображающего одноразовый пароль, и т. д.

Двухфакторная аутентификация (англ. Two-factor authentication) – порядок аутентификации пользователя, при котором проверяются не менее двух факторов. В числе этих факторов: обладание предметом (например, аппаратным или программным токеном); обладание информацией (например, паролем, парольной фразой или ПИН-кодом); обладание пара-

метрами или навыками (например, отпечатками пальцев или другими биометрическими параметрами) [16].

Биометрическая идентификация/аутентификация (англ. Biometrics identification/authentication) – аутентификация или идентификация посредством предоставления человеком своих физиологических параметров (например, отпечатки пальцев, радужная оболочка глаза, сетчатка глаза и т. д.).

Контроль доступа (англ. Access control) – механизмы, с использованием которых доступ к данным или к ресурсам для обработки данных ограничивается только авторизованным кругом лиц или приложений [16].

Целевая атака (APT-атака, англ. Advanced persistent threat (APT) – хорошо организованная, тщательно спланированная кибератака, которая направлена на конкретную компанию или отрасль.

Центр обеспечения безопасности (англ. Security operation center (SOC) – это команда, состоящая в основном из аналитиков по безопасности, в задачи которой входят обнаружение и анализ инцидентов кибербезопасности, оперативное реагирование, предотвращение их возникновения и составление отчетности.

Хакбэк (сленг, англ. Hackback) – процесс ответной атаки на злоумышленника.

Атака на цепочку поставок (англ. Supply chain attack) – тип кибератаки, при которой вредоносные функциональные возможности внедряются в цепь поставки, например в процесс разработки легального ПО.

Технические средства защиты авторских прав (англ. DRM – Digital rights management (ТСЗАП) – программные или программно-аппаратные средства, которые намеренно ограничивают либо затрудняют различные действия с данными в электронной форме (копирование, модификацию, просмотр и т. п.) либо позволяют отследить такие действия.

Криптография. Защита данных – Cryptography. Data protection

Защита данных – организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов данных или экземпляров типов данных в системе обработки данных [15].

Криптография (англ. Cryptography) – раздел математики и информатики, занимающийся безопасностью информации, в частности шифрованием и аутентификацией. В области безопасности сети и приложений является инструментом для обеспечения контроля доступа, конфиденциальности и целостности информации [16].

Шифрование (англ. Encryption) – обратимое преобразование информации в целях сокрытия ее от лиц, не обладающих специальным (криптографическим) ключом. Весь секрет заключается в ключе шифрования, но не в алгоритме шифрования, который обычно является общедоступным. Алгоритмы шифрования разделяются на симметричные, где используется один ключ для шифрования и расшифровки, и асимметричные (с открытым ключом), которые используют связанную математически друг с другом пару ключей (ключевая пара): открытый ключ (публичный) и закрытый ключ (секретный). При этом при шифровании данных открытым ключом расшифровать их возможно только с помощью соответствующего ему закрытого ключа. Алгоритм шифрования и ключи выбираются заранее участниками передачи и (или) хранения зашифрованных данных.

Стеганография – метод сокрытия самого факта хранения или передачи данных. Например, защищаемые данные могут быть спрятаны в файл изображения или аудиофайл.

Контрольная сумма (англ. Checksum) – некоторое значение, рассчитанное по определенному алгоритму (пример: алгоритм CRC32), для проверки целостности данных при их пере-

даче и хранении. В качестве контрольной суммы может быть использован результат криптографической хеш-функции.

Хеш, **хеш-сумма** (англ. Hash) – результат необратимого преобразования (с помощью хеш-функции) входного массива данных произвольной длины в выходную строку фиксированной длины. Для подтверждения подлинности и целостности (неизменности) применяются криптографические хеш-функции, к которым предъявляются требования стойкости к коллизиям (вероятности нахождения другого массива данных, имеющего идентичную хеш-сумму).

Примеры хешей от слова mypassword по алгоритму MD5 (как и SHA-1, больше не считается стойким): 9041e64114e02002e 821563757105d3a; SHA-256 – 3f15df31c6-8603c604caafabbd097 bfa6cc3459f6f8da491fe9406dfdefda187.

Примечание. Расчет контрольной суммы файла производится от его содержимого и не зависит от его наименования, временных меток и пути.

Учитывая, что от одинаковых входных значений (например, одинаковых паролей) получаются одинаковые хеши, становится возможным заранее рассчитать результат хеширования, построив радужные таблицы (англ. Rainbow table). Поиск по этим таблицам позволяет практически мгновенно находить коллизии для рассчитанных значений. Для противодействия радужным таблицам при расчете хеша к входным данным добавляется некоторое случайное значение, называемое солью (англ. Salt).

Примеры «соленых» хешей от слова mypassword, соответственно с солью «wRcQgLso» и «9cEzrciK»: 1wRcQgLso-$OHhr Z0YsSco0sQwlj4adW1 и $1$9cEzrciK$JB6lCXX9Pi7tH-8TO0W3GA0.

Полный перебор (метод «грубой силы», сленг «брут», «брутфорс», англ. Brute-force) – метод нахождения решения какой-либо задачи путем прямого перебора всех возможных решений. Методом перебора входных значений возможен поиск коллизий хеш-функции, например для получения из хеша исходного пароля.

Криптоконтейнер (англ. Encrypted container) – хранилище зашифрованных данных, как правило, представленное в виде файла.

Шифрование диска (англ. Disk encryption) – метод или технология (программная или аппаратная) для шифрования всех данных, которые хранятся на устройстве (например, на жестком диске или флеш-накопителе) [16].

Скрытый раздел (англ. Hidden volume) – второй раздел на криптоконтейнере (по аналогии со шкатулкой с двойным дном), располагаемый в свободном пространстве основного раздела, доступ к которому осуществляется по отличному от основного раздела ключу (паролю).

Цифровая подпись (ЦП, электронная цифровая подпись (ЭЦП), англ. Digital signature) – реквизит электронного документа, сформированный путем криптографического преобразования электронного документа с использованием закрытого ключа. Цифровая подпись позволяет подтвердить авторство документа, его целостность и неотказуемость.

Цифровой сертификат (криптографический сертификат, англ. Digital certificate) – электронный документ, подтверждающий принадлежность владельцу каких-либо атрибутов, в частности публичного ключа (англ. Public key certificate). В сертификате по стандарту **X.509** среди атрибутов указаны сведения о владельце сертификата, его открытом ключе, удостоверяющий центр, цифровая подпись и др. Сертификаты могут быть в текстовом формате PEM (содержимое начинается с «-- BEGIN CERTIFICATE --» и заканчивается «-- END

CERTIFICATE --», расширения файлов «.pem», «.crt» и «.cer»), бинарном формате DER (расширение файла «.der»), текстовом PKCS7/P7B (расширение файла «.p7b» или «.p7c») или бинарном PFX (PKCS12) (расширение файла «.pfx» или «.p12»).

Удостоверяющий центр (УЦ) (англ. Certificate authority) – третья сторона (организация или иной субъект), обладающая доверием, которая выпускает цифровые сертификаты и подтверждает подлинность ключей шифрования посредством электронной подписи.

Самоподписанный сертификат (англ. Self-signed certificate) – вид цифрового сертификата, подписанный владельцем данного сертификата вместо удостоверяющего центра.

Отпечаток открытого ключа (сленг «фингерпринт», англ. Fingerprint) – небольшая последовательность байтов (хеш-значение), позволяющая идентифицировать открытый ключ. Пример отпечатков: «da:19:c4:23:9c:03:de:94:69:8a:88:b0:2d:0-1:c7:14», «GZyqQIfmntSQtvVURjth8nXC9IWBdifweEE7qogZuIc».

Шифрование диска (англ. Disk encryption) – метод или технология (программная или аппаратная) для шифрования всех данных, которые хранятся на устройстве [16]. В случае шифрования всех разделов, включая загрузочный, шифрование является полнодисковым (англ. Full disk encryption (FDE). Примеры реализации: на Filevault2 в ОС MacOS, Bitlocker в ОС семейства Microsoft Windows.

Энтропия (информационная) (англ. Entropy) – мера неопределенности (беспорядка) информации, соответствующая количеству информации в передаваемых или хранимых данных. У текстовых данных энтропия низкая из-за большой определенности, так как некоторые буквы («а», «о», «е», «и» и т. д.) встречаются с большей частотой, чем другие («ы», «ш», «ц»). Высокое значение энтропии может указывать на зашифрованные или сжатые (заархивированные) данные.

OTR (сленг «отр», англ. Off-the-recording messaging) – криптографический протокол для систем обмена мгновенными сообщениями, обеспечивающий шифрование переписки между двумя участниками, а также их аутентификацию.

OpenPGP (сленг «пгп») – стандарт шифрования электронной переписки, основанный на криптографии с открытым ключом. Основан на ПО PGP (англ. Pretty good privacy). Одной из самых распространенных реализаций является GnuPG (GPG).

Менеджер паролей (англ. Password manager) – ПО, предназначенное для безопасного хранения паролей. Пароли хранятся в зашифрованном виде и становятся доступны пользователю после ввода мастер-пароля к хранилищу паролей (англ. Master password). Примеры менеджеров: KeePass, 1Password, KeyChain, LastPass.

XOR (исключающее «ИЛИ», сленг «ксор», англ. Exclusive or) – математическая (логическая) операция. Данная операция может быть использована в качестве простейшего алгоритма шифрования.

Нечеткий хеш (англ. Fuzzy hashing, Context triggered piecewise hashing (CTPH) – хеш, который изменяется не полностью (в отличие от криптографического хеша), если хешируемые данные изменились частично. Применяется для поиска похожих объектов (файлов, писем и т. д.). Изначально реализован в утилите SSDeep.

Случайное значение (сленг «рандом», англ. Random) – псевдослучайное число, генератор псевдослучайных чисел (ГПСЧ).

Атака на вычислительную систему – Attack (computing)

Тест на проникновение (сленг «пентест», англ. Penetration testing) – метод оценки защищенности информационной системы (в частности, вычислительной сети или приложения) путем попытки проведения атаки на нее под видом злоумышленника

(в соответствии с моделью нарушителя). Тестирование санкционировано владельцем информационной системы и может производиться «пентестером» как часть аудита ИБ.

Модель нарушителя (ИБ) (англ. Information security intruder model) – описание и классификация нарушителей информационной безопасности, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способа реализации угроз информационной безопасности со стороны указанных нарушителей [19].

Взломщик (сленг «хакер», англ. Hacker) – специалист по проникновению в вычислительные системы.

Хакер – Black hat (сленг «блекхат», «блек», «блечер») – некто, совершающий кибератаки в корыстных целях. Не путать с «блек»/«блеклист» (черный список), этичный хакер (white hat).

Эксфильтрация (англ. Exfiltration, сленг «граб», англ. Grab) – несанкционированное копирование данных.

Перехват сетевого трафика (англ. Network sniffing) – метод пассивного мониторинга или сбора сетевых коммуникаций, декодирования протоколов и изучения содержимого на предмет наличия интересующей информации [16].

Атака «Человек посередине» (сленг «митм», англ. Man-in-the-middle (MitM) – вид атаки, при которой злоумышленник перенаправляет через себя данные, передаваемые двумя сторонами друг другу, тем самым получая доступ к содержимому с возможностью их модификации.

Атака на отказ в обслуживании (сленг «дос», англ. Disk Operating System (DoS) – атака, при которой нарушается доступность вычислительной системы для ее пользователей.

Распределенная атака на отказ в обслуживании (сленг «ддос», англ. Distributed Denial of Service (DDoS) – атака на отказ в обслуживании, которая осуществляется одновременно с разных сетевых узлов (посредством «ботнета», через скомпро-

метированные сетевые ресурсы, сторонние уязвимые сетевые сервисы, с бытовых приборов из «Интернета вещей» и т. д.).

Инъекции (англ. Injection flaws) – уязвимость, возникающая в результате небезопасных методов программирования, выражающихся в некорректной проверке введенных данных, которая позволяет злоумышленникам передать в нижележащую систему вредоносный код через веб-приложение. Данный класс уязвимостей включает, например, SQL-инъекцию, инъекцию LDAP и инъекцию XPath [16].

SQL-инъекция (сленг «скуль», англ. SQL injection) – тип атаки на веб-сайт с базой данных. Злоумышленник выполняет несанкционированные команды SQL, применяя их к небезопасному коду в системе, подключенной к сети Интернет. SQL-инъекции используются для кражи из базы данных информации, к которой при обычных условиях отсутствует доступ, и (или) для получения доступа к хост-машинам организации через компьютер, на котором размещена база данных [16].

Межсайтовый скриптинг (XSS, англ. Cross-site scripting) – уязвимость, возникающая в результате небезопасных методов программирования, выражающаяся в некорректной проверке введенных данных [16].

Подмена IP-адреса (сленг «спуфинг», англ. IP address spoofing) – метод атаки, используемый для получения несанкционированного доступа к сетям или компьютерам. Злоумышленник направляет компьютеру ложные сообщения с IP-адресом, указывающим на доверенный хост в качестве источника сообщения [16].

Дефейс (англ. Deface) – изменение внешнего облика вебсайта в целях демонстрации полученного к нему несанкционированного доступа.

Социальная инженерия (СИ, англ. Social engineering) – метод манипулирования поведением человека в целях выполнения им действий в интересах инициатора.

Фейк (англ. Fake) – применительно к социальной инженерии поддельный объект (письмо, окно приложения, веб-сайт, «скан» паспорта и т. д.), имитирующий оригинал.

Ханипот (англ. Honeypot) – сетевой узел (ресурс), представляющий собой специально приготовленную приманку для злоумышленников.

Intrusion detection system (IDS) и Intrusion prevention system (IPS) – системы обнаружения (СОВ) и предотвращения вторжений (соответственно), в частности обеспечивающие защиту от сетевых атак и несанкционированного доступа. Система IPS дополнительно позволяет активно противостоять сетевой атаке (блокировать). Системы IDS и IPS могут использоваться совместно с антивирусами.

Сетевой сканер (сканер портов, англ. Network scanner) – утилита, позволяющая определить открытые сетевые порты на удаленном сетевом узле посредством отправки различных сетевых пакетов, в частности путем попытки установления соединения. Наиболее популярным сетевым сканером является Nmap.

Сканирование сети на наличие уязвимостей (Network security scan) – процесс, позволяющий ручными или автоматизированными средствами выполнять удаленную проверку систем организации на наличие уязвимостей, который включает в себя тестирование внешних и внутренних систем, а также предоставление отчетов о службах, доступных по сети. Сканирование может выявлять уязвимости в ОС, службах и устройствах, которыми могут воспользоваться злоумышленники [16].

Веб-шелл (сленг «шелл», англ. Web shell) – веб-приложение (обычно представленное в виде одного файла), предоставляющее управление над системой (выполнение команд в ОС, операции с файловой системой и т. д.), на которой работает веб-сервер с этим веб-шеллом. Веб-шеллы использу-

ются злоумышленниками для несанкционированного доступа, полученного, в частности, через уязвимости в веб-приложениях.

Metasploit Framework (MSF) («метасплоит») – программный комплекс для разработки и применения эксплоитов. MSF содержит большой набор готовых вспомогательных утилит (англ. Auxilary), эксплоитов и «полезных нагрузок», позволяющих находить и эксплуатировать уязвимости в вычислительных системах. Несмотря на предназначение комплекса для использования в рамках тестирования защищенности, в частности в тестах на проникновение, данный комплекс пользуется популярностью у злоумышленников для получения несанкционированного доступа.

Meterpreter (сленг «метер», «метерпретер») – полезная нагрузка (payload), входящая в состав Metasploit Framework, обладающая широкими функциональными возможностями.

Cobalt Strike (сленг «кобальт») – программный комплекс, подобный Metasploit Framework, использующий более продвинутые «полезные нагрузки», называемые «биконами» (англ. Beacon).

Кибербразведка (англ. Cyber threat intelligence (CTI) – сведения об актуальных киберугрозах и их источниках. Сведения собираются, обрабатываются и анализируются для понимания мотивов, целей и методов противника (англ. Threat actor).

Поиск угроз (англ. (Cyber) Threat Hunting (TH) – практика проактивного поиска киберугроз, которые еще не были обнаружены.

Разведка на основе открытых источников (англ. Open source intelligence, OSINT) – разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также ее анализ.

CERT (англ. Computer Emergency Response Team) – группа реагирования на компьютерные инциденты, представляющая собой независимую группу экспертов, в список задач которой

входят постоянный мониторинг информации о появлении угроз в сфере информационной безопасности (ИБ), их классификация и нейтрализация.

Красная команда (сленг «редтим», англ. Red team) – вариант учений, имитирующих реальные кибератаки, при которых действуют две группы – атакующая и защищающая – красная команда и синяя команда (англ. Blue team) соответственно. Гибрид обеих команд называется пурпурной командой (англ. Purple team).

Захват флага (англ. Capture the flag (CTF) – вид командных соревнований по кибербезопасности, при которой участники должны защищать свой сервер и атаковать серверы других участников. Также соревнования могут проводиться в формате отдельных заданий.

Компьютерная криминалистика – Computer forensics

Форензика (англ. Computer forensics) – в русскоязычной среде компьютерная криминалистика. Форензика – цифровая криминалистика + DFIR (Incident response – комплекс мероприятий по реагированию на инцидент информационной безопасности).

Образ оперативной памяти («дамп памяти», «снимок памяти», англ. Memory dump). Это последовательность инструкций машинного кода и связанных с ними данных, постоянно хранящихся в энергонезависимой памяти ПЗУ встроенной системы, которая копируется в энергозависимую оперативную память загрузчиком начальной загрузки. Снимок памяти – содержание рабочей памяти процесса, ядра или всей ОС в определенный момент времени. Может быть использован для анализа запущенных программ и выявления ошибок (отладки), а также для получения данных, обрабатываемых указанными программами.

Дупликатор (англ. Duplicator) – устройство, позволяющее сделать посекторную копию (образ) с накопителя данных, не внося изменений в оригинальный накопитель. Дополнительно может быть рассчитана контрольная сумма от полученного образа.

Блокиратор записи (англ. Write blocker) – устройство, позволяющее производить чтение с накопителя данных, при этом предотвращающее операции записи на него («в режиме чтения», англ. Read-only (RO).

Образ диска (англ. Disk image) – файл, содержащий полную копию данных или копию логического раздела с накопителя данных (НЖМД, флеш-накопителя, оптического диска и т. д.). Для криминалистических целей распространены образы в формате Encase (EWF). Также образ может быть получен в «сыром» виде (RAW), содержащем данные без сжатия и метаданных. Образ может быть разбит на несколько файлов для записи на несколько носителей или из-за ограничений файловой системы (FAT32 не поддерживает файлы размером более 4 Гб).

EWF (формат Encase, англ. EnCase image file format) – формат файла, предназначенный для хранения цифровых доказательств (образа накопителей данных, логических разделов, оперативной памяти или отдельных файлов). Формат поддерживает сжатие данных, шифрование и содержит метаданные, включающие информацию об объекте и его контрольные суммы. Файлы имеют расширение «.E01», «.E02» и т. д.

Безопасное удаление данных (сленг «вайп», англ. Secure wipe) – метод перезаписи данных на жестком диске или другом цифровом носителе, исключающий возможность восстановления данных [16].

Ложно-позитивная ошибка (ошибка 1-го рода, сленг «фолса», англ. False positive) – ошибка, при которой происходит ложное срабатывание. Пример: признание невиновного виновным.

ГЛАВА 8. ФИНАНСОВАЯ ТЕРМИНОЛОГИЯ

Банковские технологии

Дистанционное банковское обслуживание (ДБО) (Банк-Клиент (сленг «БК») – общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом. Может быть выполнен в виде отдельного приложения («Толстый клиент») или вебсайта («Тонкий клиент», интернет-банк).

Интернет-банк (сленг «онлайн», «онлик») – см. ДБО.

Антифрод (англ. Anti-Fraud, сленг «фрод» (англ. Fraud – мошенничество) – комплекс мер, принимаемых кредитными организациями, направленных на противодействие сомнительным финансовым операциям.

БС – банковская система.

АБС – автоматизированная банковская система.

БЭСП – банковская электронная система платежей (быстрые платежи).

АРМ КБР (автоматизированное рабочее место клиента Банка России) – ПО для управления корреспондентским счетом и обмена информации с Банком России. Также называется рабочее место (ПК), на котором данное ПО установлено и осуществляется связь с Банком России.

ОКВЭД – Общероссийский классификатор видов экономической деятельности.

Платежные реквизиты (сленг «реки», «реквы», «рек») – сведения, необходимые для перечисления денежных средств.

Платежное поручение (ПП) – распоряжение владельца счета о перечислении денежных средств кредитной организации (банку). В случае электронного платежного поручения может иметь различные статусы (в зависимости от конкретной АБС) в процессе исполнения, например: «принято», «обрабатывается», «выполнено», «исполнено», «отказано» и т. д.

Операционные часы (сленг «оперчасы») – время работы, в которое кредитная организация осуществляет обслуживание клиентов, в том числе время, в течение которого принимает и исполняет платежные поручения.

Холдер («держатель», англ. Holder) – владелец банковского счета.

SWIFT (свифт, англ. Society for Worldwide Interbank Financical Telecommunications) – международная межбанковская система обмена информацией о финансовых операциях.

IBAN (англ. International Bank Account Number) – международный номер банковского счета.

Электронная платежная система (система электронных платежей, англ. E-commerce payment system, Electronic payment system) – сервис, предоставляющий возможность дистанционного осуществления платежей. Примеры распространенных электронных платежных систем: PayPal (сленг «палка»), Western Union (WU), «Контакт», Qiwi, WebMoney (WM).

Децентрализованные финансы (англ. Decentralized finance, DeFi) – общее название для аналогов традиционных финансовых инструментов, реализованных в децентрализованной архитектуре в виде **децентрализованного приложения** (англ. decentralized application (DApp), которые обычно основаны на смарт-контрактах.

Смарт-контракт (умный контракт, англ. Smart contract) – программный код, хранимый в блокчейне и автоматически исполняющий все условия соглашения (контракта). Смарт-контракты для платформы Ethereum пишутся на языке Solidity.

Несанкционированное списание денежных средств

Кэш (сленг, англ. Cash) – наличные деньги.

Селлер (сленг, англ. Seller) – продавец чего-либо (например, платежных карт, «дроп-контор»).

Гарант (сленг) – лицо, пользующееся авторитетом у участников сделки, которое за некоторое вознаграждение следит за выполнением ее условий каждой из сторон.

Регистратор («регер») – лицо, осуществляющее регистрацию юридических лиц, индивидуальных предпринимателей (ИП), а также открытие расчетных счетов в кредитных организациях.

Залив (сленг «лить», «заливать», «ставить», «грузить», «пулять») – осуществление платежа, несанкционированного уполномоченным лицом. Может производиться вручную (формирования платежного поручения) или автоматизированно (автозалив (АЗ), с использованием специального ПО. Может осуществляться путем скрытой подмены реквизитов получателя.

Заливщик – физическое лицо, осуществляющее действия, приводящие к выполнению финансовых операций (платежей), несанкционированных уполномоченным лицом (см. Залив).

Дроп (устар. «мул», англ. Drop, Mule) – подконтрольный посредник, участвующий в финансовых операциях в целях затруднения отслеживания конечных участников данных операций (бенефициаров). Некорректно – «дроппер» (см. Классификация ВПО).

Обнальщик (нальщик) – лицо, осуществляющее обналичивание денежных средств. Могут быть как «белые» (сленг «с реала», «реальный»), занимающиеся «коммерческим» обналом, так и «черные», занимающиеся приемом и обналичиванием несанкционированно списанных денежных средств.

Грязь (сленг) – несанкционированно списанные денежные средства.

Долить (сленг «докинуть») – осуществить повторный «залив» с одного и того же лица (до того, как «спалили» первый «залив»).

Зависнуть (сленг «завешивать») – блокировать (со стороны кредитной организации) денежные средства, поступившие на расчетный счет дропа («приемной лавки»).

Блокировка расчетного счета (сленг «лок», «блок») – ситуация, при которой кредитная организация накладывает (налагает) ограничения на операции с расчетным счетом клиента.

Единичка (сленг «1кк») – один миллион (сленг «лям», «лимон») в любой валюте, где под «1к» подразумевается 1 000 (сленг «кило»).

Выплата (сленг) – перечисление нальщиком доли от обналиченных денежных средств («грязи») заливщику.

Ноги (сленг «прийти с ногами», «пришли ноги») – запрос или предписание в кредитную организацию от каких-либо официальных органов (правоохранительных и налоговых органов, судебных приставов-исполнителей).

Удержать (сленг «удержание») – запас времени, имеющийся у злоумышленников до момента блокировки расчетного счета банком (насколько банк «дает работать» / «дает грузить»).

Палить (сленг) – обнаружить (как правило, владельцем счета) какие-либо несанкционированные действия («спалить»).

Депозит (сленг) – исполнить обязательства нальщика перед заливщиком путем предоставления согласованной суммы денежных средств заливщику или гаранту.

Приемная фирма (сленг «лавка», «приемная контора», «дроп», «приемная лавка», «прокладка», «контор», «фирма», «юр», «юрик», «корп») – юридическое лицо, используемое для «**приема залива**» и последующего обналичивания либо транзита денежных средств на следующий элемент обнальной цепочки. Пример: на приемную фирму «залетает»/«зачисляется»/«заходит»/«падает» «грязь», а затем «выходит»/«раскидывает»/«списывается»/«выводится» на следующую «лавку» либо «сналивается».

Внутрибанковский платеж (сленг «внутрибанк») – платеж, осуществляемый внутри одной кредитной организации.

Межбанковский платеж (сленг «межбанк») – платеж, осуществляемый между счетами в разных кредитных организациях.

Кэш-карта (англ. Cash-Card) – банковский продукт, платежная карта, позволяющая вносить на счет организации (к которой привязана карта) и снимать наличные денежные средства.

Разгонять (сленг «раскидывать») – выводить денежные средства с «приемной лавки» на последующие звенья цепи обнала в целях уменьшения риска блокировки счета до полного обналичивания «слитых» денежных средств.

Работа внутри банка (сленг) – вывод денежных средств («разгон») осуществляется на расчетные счета в этой же кредитной организации («внутрибанк») или через ее же платежные карты.

Прокачивать корпа (сленг «качать корпа», «создавать оборот») – осуществлять легальные («белые») платежи для увеличения оборота по расчетному счету («лавки»/«конторы») в целях уменьшения риска блокировки подозрительных операций кредитной организации (обхода банковских систем – «антифрода») посредством имитации нормальной (обычной) хозяйственной деятельности.

Чистая контора / ИП (сленг) – юридическое лицо или индивидуальный предприниматель, которые ранее не участвовали в приеме «заливов», транзите либо обналичивании денежных средств («контора, через которую не проходила грязь»).

Прозвон (сленг) – проверка сотрудником кредитной организации или торгово-сервисного предприятия санкционированности/легитимности осуществляемой финансовой операции посредством телефонного звонка.

115 (сленг) – Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма)».

Материал (сленг) – все, что связано с обналом. Используется в процессе залива и обнала: платежные карты, «фирмы», «конторы», «лавки». Пример: «расходовать материал».

Ходун (сленг «бегунок») – лицо, осуществляющее непосредственное снятие наличных (в «поле») в банкомате или кредитном учреждении.

Кэш-ин (сленг, англ. Cash In) – банкоматы или платежные терминалы с функцией внесения наличных денежных средств для зачисления на счет.

Бух/дир/гена (сленг) – обозначение должностей бухгалтера, директора и генерального директора соответственно.

Печатка (сленг «штамп», «штампик») – образец печати (штампа).

Крючок (сленг) – образец подписи.

Платежные карты, мошенничество с платежными картами – Payments cards, Credit card fraud

Мошенничество с платежными картами, **Кардинг** (англ. Carding) – вид мошенничества, при котором осуществляются несанкционированные владельцем платежной карты операции, связанные с картой или ее реквизитами.

Кредитная карта (сленг «картон», «кредитка», «сс», англ. Credit card (CC) – платежная карта или ее реквизиты. Кредитной картой также в разговорной речи могут называться дебетовые карты.

Белый пластик (сленг) – заготовка для платежной карты, представляющая собой неперсонализированную пластиковую карту (обычно белого цвета) с магнитной полосой.

Номер карты (сленг «пан», англ. Primary account number (PAN) – уникальный номер платежной карты (как правило, кредитной или дебетовой), который идентифицирует эмитента и соответствующий счет держателя карты. Обычно номер карты состоит из 16 цифр (может быть от 12 до 19), первые 6 указывают на банк-эмитент (сленг «бин», англ. BIN (Bank identification number) / IIN (Issuer identification number), а последние являются контрольной суммой, рассчитываемой по алгоритму Луна (англ. Luhn algorithm).

Данные платежных карт (англ. Account data) – это сведения о держателе карты и (или) критичные аутентификационные данные [15].

Данные магнитной полосы, **Трек** (англ. Magnetic stripe data, Track) – данные, записанные на магнитной полосе или чипе, которые используются для аутентификации и (или) авторизации при платежных транзакциях [15]. На пластиковых картах магнитная полоса состоит из трех треков (дорожек), при этом для платежных операций обычно используется трек № 2.

Код проверки подлинности карты (значение подтверждения подлинности карты, англ. Card verification code 2 (CVC2), Card verification value 2 (CVV2) – трехзначное число (для карт American Express – четырехзначное), напечатанное на оборотной стороне платежной карты и используемое при проведении операций без присутствия карты (англ. Card not present transaction, CNP), в частности при проведении платежей через Интернет.

Держатель карты (сленг «картхолдер», англ. Cardholder) – клиент или работник, на имя которого выпущена платежная карта, или любое лицо, имеющее право пользоваться платежной картой [16].

Смарт-карта (умная карта, чиповая карта, чипованная карта, англ. Smart card, Chip card) – тип платежной карты, которая имеет встроенный микропроцессор. Микропроцессор (чип) со-

держит данные платежной карты, включая, среди прочих, данные, эквивалентные данным магнитной полосы [16].

Процессинговый центр (ПЦ, сленг «процессинг», англ. Payment processor) – организация или подразделение организации, осуществляющие обработку (процессинг) операций с использованием платежных карт.

Банкомат (сленг «атм», англ. Automated teller machine (ATM) – устройство, позволяющее владельцам платежных карт выполнять финансовые операции.

POS (сленг «пос», «терминал», англ. Point of sale) – аппаратное и (или) ПО, которое используется для обработки транзакций с платежными картами на территории торгово-сервисного предприятия [15].

Эмитент (англ. Issuer) – организация, которая выпускает платежные карты, оказывает (содействует в оказании) или поддерживает услуги выпуска карт. К таким организациям относятся, среди прочего, банки-эмитенты и эмиссионные процессинговые центры. Синоним: «банк-эмитент» (Issuing bank) или «финансовая организация – эмитент» (Issuing financial institution) [15].

Эквайрер (англ. Acquirer) – организация, которая устанавливает и поддерживает договорные отношения с торгово-сервисными предприятиями по приему платежных карт. Синонимы: «банк торгово-сервисного предприятия» (Merchant bank), «банк-эквайрер» (Acquiring bank), «финансовая организация – эквайрер» (Acquiring financial institution) [15].

Скиммер карт (англ. Card skimmer) – физическое устройство (часто подсоединяемое к легитимному устройству, используемому для считывания информации с платежных карт), предназначенное для незаконного считывания и (или) сохранения информации с платежной карты [15].

Энкодер (англ. Encoder) – устройство, позволяющее записывать данные на магнитные полосы пластиковых карт.

Карженый (сленг) – товар или услуга, оплаченные с помощью реквизитов скомпрометированной платежной карты.

Криптовалюты – Cryptocurrency

Криптовалюта (англ. Cryptocurrency) – цифровая (электронная) валюта, работа которой основана на криптографических алгоритмах. Криптовалюта – криптомонета/токен.

Биткоин (сленг «биток», «бтс», «бтц», англ. Bitcoin (BTC) – первая децентрализованная криптовалюта, являющаяся одной из самых распространенных.

Блокчейн (англ. Blockchain) – распределенная база данных, представленная в виде набора блока данных, каждый из которых зависит от предыдущего. В криптовалютах блокчейн используется для хранения информации о совершенных транзакциях.

Сатоши (англ. Satoshi) – самая маленькая единица биткоина, равна 0,000 000 01 BTC.

Фиатные (декретные) деньги (сленг «фиат», англ. Fiat money) – деньги, номинальная стоимость которых устанавливается и гарантируется государством.

Альткоин (англ. Altcoin) – собирательное название для криптовалют, отличных от биткоина.

Майнинг (добыча) (англ. Mining) – процесс получения криптовалюты в виде вознаграждения в процессе поддержания работы инфраструктуры данной криптовалюты.

Майнер (англ. Miner) – лицо или ПО, осуществляющее майнинг криптовалюты.

Обменник (сленг) – сервис по обмену традиционных, электронных и других типов валют (криптовалют).

Криптокошелек (англ. Cryptocurrency wallet) – устройство («холодный» кошелек), физический носитель или онлайн-сервис («горячий» кошелек), который хранит публичный и

(или) закрытый криптографические ключи для проведения операций с криптовалютой.

Криптовалютный миксер (англ. Cryptocurrency tumbler, cryptocurrency mixing service) – сервис, позволяющий запутать финансовые потоки криптовалюты, тем самым усложняя отслеживание транзакций.

Ethereum (Эфириум, сленг «эфир») – криптовалюта и платформа для создания децентрализованных онлайн-сервисов блокчейна (децентрализованных приложений), работающих на базе умных контрактов.

ГЛАВА 9. ЖАРГОН, СЛЕНГ

Сокращения, используемые в переписке (в алфавитном порядке)

btw (англ. By the way) – кстати, между прочим.

fyi (англ. For your information) – к вашему сведению.

thx (англ. Thanks) – спасибо.

til (англ. Today i learned) – сегодня я узнал.

tl; **dr** (англ. too long; didn't read – слишком длинно, не читал) – используется как подзаголовок для краткого резюме.

асап (asap, англ. As soon as possible) – как можно скорее.

афаик (afaik, англ. As far as i know) – насколько мне известно.

афк (afk, англ. Away from keyboard) – отошел (от клавиатуры).

бб (bb, англ. bye-bye) – прощание («пока»), окончание переписки.

бро (bro, сокращение от «брат», англ. Brother) – форма обращения к собеседнику.

втф (wtf, англ. What the fuck) – какого черта?

зы – p.s. (в некорректной раскладке).

имхо (imho, англ. In my humble opinion) – по моему скромному мнению.

кек – обозначение (ироничного) смеха.

кк – ок, хорошо, принято.

ку (re, q) – приветствие.

лол (lol, англ. Laughing out loud) – выражение смеха.

омг (omg, англ. Oh my god) – о боже.

плиз (plz, англ. Please) – пожалуйста (просьба о помощи).

рофл (rofl, англ. Rolling on the laughing floor) – выражение смеха.

ртфм (rtfm, англ. Read the fucking manual) – прочитай мануал (инструкцию).

сабж (subj, англ. Subject) – слово, указывающее на тему переписки, сообщения (поста), тикета и т. д.

хз (hz) – не знаю, не обладаю информацией.

Сленг, жаргонизмы (в алфавитном порядке)

Аксес, Аксцес (сленг, англ. Access) – доступ.

Аплоад/даунлоад (англ. Upload/download) – загрузка на/с удаленного сетевого узла (например, сервера, веб-сайта).

Варез (англ. Warez) – пиратское, крякнутое ПО.

Вес – размер файла, объем хранимых данных.

Весить, вес – описание размера данных или файла. Пример: «файл весит 3 метра», значит «размер файла – 3 мегабайт».

Глюк (глючит) – описание некорректной работы программы или вычислительного устройства.

Девайс (англ. Device) – устройство.

Дисконнект (англ. Disconnect) – отключение, прерывание соединения.

еу, ру, ус, ук, де, уа (eu, ru, us, uk, de, ua и т. д.) – условное обозначение геополитического признака (стран и регионов) для Евросоюза (EU), Российской Федерации (RU), США (US), Великобритании (UK), Германии (DE), Украины (UA) соответственно. Используется для указания целевой аудитории.

Кастомный (англ. Custom) – нестандартный, сделанный под конкретный случай.

Кидала – мошенник, аферист; человек, умышленно нарушивший условия договора.

Конферм, конфирм (англ. Confirm) – подтверждение чего-либо.

Копипаст (англ. Copy-paste) – обозначение операции по копированию текста и последующей его вставке.

Крутится – работает, выполняет свои функции. Пример: крутится веб-сервер.

Ламер (англ. Lamer) – лицо, плохо разбирающееся в компьютерной технике.

Мануал (англ. Manual) – руководство по применению, инструкция по эксплуатации.

Матчить (англ. Match) – сопоставлять что-либо, сравнивать.

Мерджить (англ. Merge) – соединять/сливать что-либо.

Метр – обозначение мегабайта. Пример: «файл весит 3 метра».

Нуб (noob, англ. Newbie) – новичок, неопытный.

Паблик (англ. Public) – 1) общедоступный; 2) публичная страница (применительно к социальным сетям).

Павн, **пвн**, **павнинг** (pwn, англ. Pawn) – обозначение овладения чем-то (получение контроля).

Прон (англ. Pron) – обозначение порнографии.

Рандом (англ. Random) – случайное значение (число).

Репа (англ. Rep, Reputation) – репутация.

Респект (уважуха, англ. Respect) – выражение уважения.

Рип (англ. Rip) – копия чего-либо, сделанная с другого формата.

Риппер, **рипак** – см. Кидала.

Рулит, **рулез** (англ. Rule, Rules) – выражение одобрения.

Скам (англ. Scam) – мошенничество.

Скан (англ. Scan) – отсканированный документ (например, «скан» паспорта).

Скилл (англ. Skill) – навык.

Скрипт-кидди (англ. Script kiddie) – унизительное название для взломщика, использующего готовое ПО и эксплоиты, не понимающего принцип их работы.

Смещение (адрес, оффсет, англ. Offset) – целое число, указывающие расстояние (смещение) от начала данных до определенного элемента этих данных.

Табуляция (Таб, англ. Tab key, tabular / tabulator key) – управляющий символ (обозначается как «\t», код символа 0x09) и одноименная клавиша на клавиатуре, используемые для горизонтального выравнивания текста.

Уронить – привести что-то (ненамеренно) в неработоспособное состояние. Пример: «уронить сервак».

Форматнуть (отформатировать, англ. Format) – процесс создания файловой системы на накопителе данных. Может сопровождаться перезаписыванием данных на накопителе без возможности их последующего восстановления (полное форматирование).

Фотошоп (фотожоп, отфотошопить, англ. Photoshop) – распространенный графический редактор. Популярен при подделке документов (см. Скан).

Функционал (фича) – функциональность, функциональные возможности (англ. Functionality, Functional capabilities).

ЦП (англ. Child pornography (CP) – материалы порнографического характера с участием несовершеннолетних лиц.

Чекать (англ. Check) – осуществлять проверку чего-либо (например, поступление денежных средств).

Шарить (англ. Share) – делиться, выкладывать в общий доступ.

Шоп (англ. Shop) – обозначение площадки (веб-сайта) или сервиса по продаже чего-либо (в частности, продажа нелегальной продукции).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Государственная Дума Федерального Собрания Российской Федерации. – URL: https://duma.consultant.ru/page.aspx?878565 (дата обращения: 02.06.2022).

2. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 02.06.2022).

3. Приказ Минкомсвязи России от 31 декабря 2015 г. № 621 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных» // НПП «КонсультатПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_194404/ (дата обращения: 02.06.2022). – Режим доступа : по расписанию.

4. ГОСТ Р 57429–2017. Судебная компьютерно-техническая экспертиза. Термины и определения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2017 г. № 198-ст : введен впервые : дата введения 2017-09-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200144960 (дата обращения: 02.06.2022).

5. ГОСТ 33707–2016 (ISO/IEC 2382:2015). Информационные технологии. Словарь : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 28 июня 2016 г. № 49) : введен впервые : дата введения 2017-09-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200139532 (дата обращения: 02.06.2022).

6. ГОСТ Р 56545–2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1180-ст : введен впервые : дата введения 2016-04-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200123701 (дата обращения: 02.06.2022).

7. ГОСТ Р 52653–2006. Информационно-коммуникационные технологии в образовании : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 419-ст : введен впервые : дата введения 2008-07-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200053103 (дата обращения: 02.06.2022).

8. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст : введен впервые : дата введения 2008-02-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 02.06.2022).

9. ГОСТ Р 53113.1–2008. Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 531-ст : введен впервые : дата введения 2009-10-01 // АО «Кодекс». – URL:

https://docs.cntd.ru/document/1200075568 (дата обращения: 02.06.2022).

10. Р 50.1.056–2005. Техническая защита информации. Основные термины и определения // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200044768 (дата обращения: 02.06.2022).

11. ГОСТ 15971–90. Системы обработки информации. Термины и определения : государственный стандарт СССР : издание официальное : утвержден и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. № 2698 : введен впервые : дата введения 1992-01-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200015664 (дата обращения: 02.06.2022).

12. ГОСТ 25868–91. Оборудование периферийное систем обработки информации. Термины и определения : межгосударственный стандарт : издание официальное : утвержден и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 28 декабря 1991 г. № 2253 : взамен ГОСТ 25868–83 : дата введения 1993-01-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200015782 (дата обращения: 02.06.2022).

13. ГОСТ 19781–90. Обеспечение систем обработки информации программное. Термины и определения : межгосударственный стандарт : издание официальное : утвержден и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 августа 1990 г. № 2467 : взамен ГОСТ 19781-83 и ГОСТ 19.004–80 : дата введения 1992-01-01 // АО «Кодекс». – URL: https://docs.cntd.ru/docu-ment/1200007684 (дата обращения: 02.06.2022).

14. ГОСТ 20886–85. Организация данных в системах обработки данных. Термины и определения : межгосударственный

стандарт : издание официальное : утвержден и введен в действие постановлением Государственного комитета СССР по стандартам от 31 января 1985 г. № 240 : взамен ГОСТ 20886-75 : дата введения 1986-07-01 // АО «Кодекс». – URL: https://docs.cntd.ru/document/1200015708 (дата обращения: 02.06.2022).

15. Глоссарий. Основные определения, аббревиатуры и сокращения. // PCI Security Standards Council. – URL: https://www.pcisecuritystandards.org/glossary/ (дата обращения: 02.06.2022).

16. Методический документ. Меры защиты информации в государственных информационных системах // АО «Кодекс». – URL: https://docs.cntd.ru/document/499083160/titles/A8I0N (дата обращения: 02.06.2022).

17. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014». // АО «Кодекс». – URL: https://docs.cntd.ru/document/499099589 (дата обращения: 02.06.2022).

18. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю. URL: https://bdu.fstec.ru/ (дата обращения: 03.06.2022).

19. ISO/IEC/IEEE 24765:2017. Systems and software engineering – Vocabulary. 2nd ed. Geneva: IEEE, 2017. https://ieeexplore.ieee.org/document/8016712 (дата обращения: 02.06.2022).

Справочное издание

Чекунов Игорь Геннадьевич,
кандидат юридических наук, доцент

Пузарин Андрей Валерьевич

Гончар Владимир Владимирович,
кандидат юридических наук, доцент

Рядовский Игорь Анатольевич

Сабитов Руслан Равильевич

Клишина Наталья Егоровна

Галиев Денис Вадимович

Справочник терминов и жаргонизмов для расследования преступлений в сфере информационных технологий

Редактор *Чамарова Н. В.*
Корректор *Мирзоева Л. С., Титова В. П.*
Компьютерная верстка *Мирзоева Л. С.*

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12

Подписано в печать 21.03.2022	Формат 60×84 1/16	Тираж	109 экз.
		1-й завод	78 экз.
Заказ № 65	Цена договорная	Объем	3,88 уч.-изд. л.
			6,10 усл. печ. л.