Общество с ограниченной ответственностью
«Информационно – консультационный учебный центр
дополнительного профессионального образования
«Профстандарт»
(ООО «ИКУЦ ДПО «Профстандарт»)

УТВЕРЖДАЮ:

Директор ООО «ИКУЦ ДПО «Профстандарт»
_____ А.Ю. Шульженко
"25" июля 2022 г.
Приказ № 21 от 25.07.2022 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПО ТЕМЕ
«Информационная безопасность»

СОГЛАСОВАНО
Зам. директора по учебно-методической работе
_____Евстифеев Р.И.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0161CBC0001CAFCEAC4D9FE835607CA475
Владелец: ШУЛЬЖЕНКО АНЖЕЛИКА ЮРЬЕВНА
Действителен: с 26.09.2022 до 26.12.2023

Мурманск
2022

План дополнительной профессиональной программы

1. **Цель изучения программы, организационно-педагогические условия ее реализации**
2. **Планируемые результаты обучения**
3. **Учебный план**
4. **Рабочая программа**
5. **Глоссарий**
6. **Список литературы**
7. **Итоговый тест**

1. **Цель изучения программы, организационно-педагогические условия ее реализации**

Цель изучения программы «Информационная безопасность»**:**
- изучение методов комплексной защиты и предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

Организационно-педагогические условия

Категория слушателей: специалисты по защите информации и должностные лица, ответственные за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса.

Срок обучения: 72 часа

Форма обучения: определяется совместно с образовательной организацией и Заказчиком (без отрыва от производства, с частичным отрывом от производства, то есть – очно-заочная форма, с применением дистанционных образовательных технологий)

Режим занятий: определяется совместно с Заказчиком (не менее 4 часов в день)

Календарный учебный график: составляется по мере набора учебных групп

Контроль проверки знаний: итоговый тест

Условия реализации педагогического процесса:
Образовательный процесс осуществляется на основе учебного плана, разработанного в соответствии с действующим законодательством. Обучение проходит очно-заочно, с использованием дистанционных образовательных технологий.
Разделы программы изложены в учебном плане. Объем разделов программы и их расположение связаны не только с действующими нормами и правилами, но и с необходимостью системного охвата изучаемых вопросов.

2. Планируемые результаты обучения по дополнительной профессиональной программе

Процесс обучения проводится очно-заочно, с применением дистанционных образовательных технологий, организовывается работа с методическими и справочными материалами, с применением технических средств обучения.
В результате освоения данной дополнительной профессиональной программы слушатель **должен знать:**

- нормативно-правовую базу в области информационной безопасности;
- общие понятия и определения, используемые в вышеуказанной сфере;
- состав угроз информационной безопасности;
- стандарты в области информационной безопасности;
- подходы к классификации автоматизированных систем;
- методы комплексной защиты и предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации

Слушатель должен **иметь навыки:**

- применения методов комплексной защиты и предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации;
- контролировать выполнение требований законодательства в области информационной безопасности.

По результатам обучения окончившему курсы специалисту выдается удостоверение установленного образца, со сроком действия 5 лет.

3. Учебный план

Модуль	Наименование разделов и дисциплин	Всего ак. час
1.	**Основы информационной безопасности**	**11**
2.	**Техническая защита информации**	**11**
3.	**Защита информации с использованием шифровальных (криптографических) средств**	**13**
4.	**Комплексная защита объектов информатизации**	**13**
5.	**Управление информационной безопасностью**	**11**
6.	**Защита в чрезвычайных ситуациях**	**11**
	Итоговая аттестация	**2**
	ИТОГО	**72**

4. Рабочая программа
курса повышения квалификации в объеме 72 академических часов по теме **«Информационная безопасность»**

Модуль 1. Основы информационной безопасности

Теория информационной безопасности и методология защиты информации. Правовое, нормативное и методическое регулирование деятельности в области защиты информации. Правовые основы организации защиты государственной тайны, задачи органов защиты государственной тайны.

Модуль 2. Техническая защита информации

Угрозы и уязвимости автоматизированных информационных систем. Классификация технических каналов утечки информации. Виды уязвимостей автоматизированных информационных систем. Оценка уровня защищённости информационных систем. Методы и средства технической защиты информации.

Модуль 3. Защита информации с использованием шифровальных (криптографических) средств

Криптографические методы защиты информации. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств.

Модуль 4. Комплексная защита объектов информатизации

Информационная безопасность автоматизированных систем. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн). Особенности защиты информации, составляющей коммерческую тайну компании. Обеспечение безопасности объектов критической информационной инфраструктуры.

Модуль 5. Управление информационной безопасностью

Управление информационной безопасностью. Организация конфиденциального делопроизводства. Аудит информационной безопасности. Экономика защиты информации.

Модуль 6. Защита в чрезвычайных ситуациях

Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее.

Итоговая аттестация - экзамен (тестирование)

5. Глоссарий

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

База персональных данных – именуемая совокупность упорядоченных персональных данных в электронной форме и/или в форме картотек персональнах данных.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Владелец баз персональных данных – государственный орган, орган местного самоуправления, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационную систему персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в

ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность - Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая).

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в т.ч. его фамилия, имя, отчество; год, месяц, дата и место рождения; адрес, семейное, социальное, имущественное положение, образование, профессия, доходы; др. информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Тёмные данные — данные, которые автоматически собираются в ходе рутинных действий в компьютерных сетях, но никоим образом не используются для получения информации или принятия решений. Способность организации собирать данные может превышать пропускную способность, с которой она может анализировать данные . В некоторых случаях организация может даже не знать, что данные собираются. По оценкам IBM, примерно 90 процентов данных, генерируемых датчиками и аналого-цифровыми преобразователями, никогда не используются.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Специальные термины

active attack – активная атака # в ИБ – атака, которая приводит к изменению функций и параметров системы или изменению данных, к нарушению интерактивных операций и взаимодействий в сети и др. Примеры подобных атак – *impersonation*, *man-in-the-middle attack*, *session hijacking* (см. также *passive attack*).

active cyberdefence (*также* **active cyber defense**, **ACD**) – активная кибероборона # проводимые в реальном времени координированные комплексные мероприятия, направленные на обнаружение, идентификацию, анализ и смягчение вредоносных последствий в случае кибератак с использованием уязвимостей компьютерной системы, сети (см. также *cyberdefence, security*).

antivirus (*также* **anti-virus**, **antivirus program**) – 1. антивирус, антивирусная программа # приложение, предназначенное для обнаружения и удаления компьютерных вирусов. Хотя даже самый лучший антивирус не может на 100% гарантировать защиту от неизвестных вирусов, тем не менее, антивирусы защищают от миллионов уже известных вредоносных программ и ими настоятельно рекомендуется пользоваться. Чтобы антивирусное ПО было эффективно, оно должно быть установлено на каждом компьютере сети. При этом следует учитывать, что антивирусы снижают общую производительность компьютерной системы. Пример: Anti-virus software consists of two parts: the scanning engine and the signature files. – Антивирусное ПО состоит из двух частей: это сканирующий движок и файлы (базы) сигнатур. Написание английского термина через дефис встречается чаще в Европе; например, desktop anti-virus – антивирус для ПК; anti-virus update – обновление антивируса (см. также *antivirus app, anti-virus policy, antivirus protection, antivirus software, signature analysis, virus, virus protection*); 2. противовирусный, антивирусный.

antivirus app – антивирусное приложение # например, antivirus app interface – интерфейс антивирусного приложения (см. также *antivirus*).

anti-virus personnel (*также* **anti-virus support personnel**) – персонал службы поддержки антивирусов # занимается установкой, обновлением и обслуживанием антивирусных программ в организации (см. также *antivirus*).

anti-virus policy – антивирусная политика # совокупность правил (политик), обеспечивающих защиту корпоративных ресурсов от вирусов (см. также *antivirus*).

antivirus protection – антивирусная защита # комплекс организационных мер и программных средств, направленных на защиту от компьютерных вирусов. Существует

множество различных вариантов антивирусной защиты. Синоним – *virus protection* (см. также *antivirus, antivirus software, malicious website*).

bacterium (*мн. ч.* **bacteria**) – бактерия, микроб # тип компьютерного вируса, последовательно саморазмножающегося и заполняющего в итоге всю систему (пожирающего её ресурсы) (см. также *virus, worm*).

bankcard fraud – мошенничество с банковскими карточками # см. также *bank card, carding, fraud.*

banker Trojan – банковский троянец, троянец для банковских систем # особая разновидность троянца, вирусного ПО, специально созданного для кражи банковских реквизитов и других конфиденциальных данных, хранящихся и обрабатываемых в онлайновых банковских системах (см. также *online banking, Trojan*).

behaviour (*брит.* **behavior**) – поведение # в ИБ, применительно к компьютерному вредоносному ПО – действия и операции, которые выполняет вредоносная программа в заражённой системе при своём запуске (см. также *malware*).

behavioural anomaly detection (**BAD**) – обнаружение аномальной активности, технология BAD # технологии обнаружения зловредного ПО, обнаружения и предотвращения НСД, основанные на анализе действий, выполняемых программой или пользователем (см. также *malver*).

behaviour blocker (*также* **behavior blocker**) – поведенческий блокиратор; блокиратор (механизм блокирования) программ с подозрительным поведением # в отличие от сигнатурных или эвристических анализаторов (входящих в состав средств ИБ) интегрируется с ОС хост-компьютера и в реальном времени следит за поведением выполняющихся программ; в случае обнаружения подозрительных действий может их заблокировать, прежде чем они нанесут вред системе, и/или удалить такую программу (см. также *behavior monitoring, heuristic analyzer, proactive security, signature*).

benign environment – благоприятная среда, защищённая среда # в ИБ – помещение, территория, зона с защитой от внешних враждебных или вредоносных элементов при помощи физических, кадровых или процедурных мер безопасности (см. также *security*).

biometric data (*также* **biometrical data**) – биометрические данные # хранимые в электронной форме данные, используемые для биометрической идентификации и/или аутентификации пользователя. Это могут быть изображения в исходном или сжатом виде либо те или иные уникальные биометрические характеристики (тембр голоса, рисунки сетчатки и радужной оболочки глаза, структура лица, форма кисти руки, отпечатки

пальцев и т. д.) (см. также *authentication, biometric authentication, biometric identification, biometric personal data, biometric sample, biometrics*).

biometric identification – биометрическая идентификация, биоидентификация # совокупность биометрических способов идентификации пользователя, основанная на уникальности характеристик человеческого тела. Например, biometric identification service – служба биометрической идентификации (см. также *biometric authentication, biometric data, biometric measurement, biometrics, fingerprint verification, identification, multimodal biometric identification*).

black hat hacker – зловредный (чёрный) хакер # синонимы – dark-side hacker, *malicious hacker* (см. также *hacker, hacking*).

blacklist (*также* **black list**) – чёрный список # *1.* в ИБ – список ресурсов, объектов, систем, хостов, приложений, которые ранее были связаны с вредоносными атаками, операциями и считаются поэтому опасными для организации, страны; *2.* записи в базе данных, перечисляющие все устройства, смарт-карты и иные объекты, которые запрещается использовать с конкретным приложением. Синоним – *negative file*; *3.* список абонентов/серверов электронной почты, которые ранее посылали спам пользователю; список доменов и/или IP-адресов сетевых объектов, хост-компьютеров, приложений, которые ранее были замечены во вредоносных или подозрительных действиях. Чёрные списки используются в системах ИБ для защиты пользователей – для блокировки поступления сообщений электронной почты с серверов или посещения сайтов, адреса которых перечисляются в этих списках; *4.* список (словарь) заранее определённых понятий, терминов, которые считаются неприемлемыми для употребления в документах, письмах организации (см. также *blacklisting, dirty word list, graylist, hotlist, whitelist*).

blacklisting – технология “чёрных списков” # в ИБ – *1.* определение списка ресурсов, объектов, систем, хостов, приложений, которые считаются подозрительными, непроверенными и небезопасными для общения, обмена данными, сообщениями и др. Одно из средств борьбы со спамом – заключается в составлении и ведении списков *DNS* подозрительных серверов (*DNSBL*), почта от которых блокируется. Метод не эффективен, так как спам в настоящее время чаще всего рассылается с “зомбированных” компьютеров, находящихся в самых разных частях планеты; *2.* обнаружение, идентификация и перечисление программ, не авторизованных для выполнения на данной компьютерной системе; *3.* выявление опасных веб-сайтов (см. также *blacklist, greylisting, whitelisting*).

blackmail – 1. шантаж, шантажирование; вымогательство # например, large-scale blackmail – крупномасштабное вымогательство. Синоним – extortion;
2. шантажировать; вымогать деньги.

botnet – *от* robot + network – сеть зомбированных компьютеров, зомби-сеть # сеть компьютеров, инфицированных вирусом таким образом, чтобы ими можно было пользоваться (управлять) удалённо, например для рассылки спама, майнинга криптовалюты или выполнения других задач и атак. Синоним – zombie army, армия зомби (см. также *botmaster, zombie computer*).

bug bounty – премия (премирование) за обнаружение уязвимости (ошибки, дефекта) # в ИБ – меры стимулирования пользователей, бета-тестеров и белых (этических) хакеров, чтобы они старались обнаруживать в аппаратных и программных продуктах уязвимости, ошибки, дефекты и сообщать о них компаниям-разработчикам этих продуктов. Компании могут за полезные результаты поощрять участников программы денежными вознаграждениями и/или награждать почётными грамотами (свидетельствами, сертификатами) (см. также *beta testing, bounty, bug, bug bounty program, ethical hacker, security, vulnerability*).

cyber attack (*также* **cyber-attack**) – кибератака, атака из киберпространства (в киберпространстве) # атака, проводимая с помощью [специальных] программных и аппаратных средств на компьютерные сети и компьютерные системы противника с целью нарушения их работоспособности или для вредоносного управления компьютерным оборудованием/инфраструктурой, либо разрушения целостности данных или завладения информацией (данными). Кибератаки – политически мотивированные или направленные на достижение чисто финансовой выгоды, – являются инструментами и составляющими кибертерроризма (*cyber-terrorism*) и киберпреступности (*cybercrime*). Например, risk of cyber attacks – риск кибератак. Синонимы – *cyber penetration, online attack* (см. также *cyber attacker, cybercrime, cybersecurity, cyberwarfare, state-sponsored online attack*).

cyber attacker – кибервзломщик – см. *attacker*.

cyberbullying – кибербуллинг # травля, оскорбления или угрозы, высказываемые жертве через социальные сети или другие средства электронных коммуникаций. Синонимы – *cyberharassment,* online bullying.

cyber conflict – киберконфликт # конфликт в киберпространстве (см. также *cyberspace, cyberwarfare*).

cybercop – 1. компьютерный полицейский, киберполицейский, киберсыщик, кибердетектив, *разг.* киберкоп # персона (или ПО), занимающаяся расследованием онлайновых преступлений или преследований (см. также *cybercrime*); 2. цензор.

cybercrime (*также* **cyber crime**) – киберпреступность, киберпреступления # литературное название преступлений, основным инструментом которых являются информационно-телекоммуникационные технологии, компьютеры и компьютерные сети. Это, например, такие традиционные преступления, как мошенничества, вымогательства (*blackmail*), хищения личных данных, но совершаемые через Интернет и/или с применением вычислительных устройств. Киберпреступность быстро стала серьёзной мировой проблемой – ввиду резкого роста числа пользователей компьютеров, смартфонов и др., и того факта, что для неё не существует никаких границ, что существенно затрудняет обнаружение и наказание киберпреступников. Отдельным видом киберпреступности является кибертерроризм. Синоним – *computer crime* (см. также также *computer criminal, criminal application, criminal attack, criminal case, criminal infrastructure, cybercop, cybercriminal, cyberlaw, cybershenanigans, cyber-terrorism, digital forensics, financial crime, fraud*, *identity theft, www.cybercrime.gov*).

cybercriminal (*также* **cyber criminal**) – киберпреступник # пример: Our goal is to be steps ahead of hackers and cybercriminals, who are attempting to exploit flaws in computer platforms and applications for their profit. – Наша цель в том, чтобы всегда на несколько шагов опережать хакеров и киберпреступников, пытающихся использовать уязвимости компьютерных платформ и приложений для своей выгоды (см. также *cybercrime*).

cybercriminal organization – кибер-ОПГ (организованная преступная группа), киберкриминальная структура (организация) # организация, занимающаяся преступной деятельностью в киберпространстве (см. также *cybercriminal*).

cyberdefense (*амер*. **cyberdefence**) – кибероборона, обеспечение кибербезопасности # см. также *cybersecurity*.

cyber detective – кибердетектив # детектив, расследующий компьютерные преступления (см. также *cybercop*).

cyber incident (*также* **cybersecurity incident**) – киберинцидент # злоумышленные действия с использованием компьютерных сетей, приводящие к реальному или потенциальному нарушению работоспособности компьютерной системы (систем) и/или разрушению (утечке, модификации и т. п.) хранящихся в ней данных (информации). Например, malicious cyber incident – вредоносный киберинцидент (см. также *cybersecurity, incident*).

cyberlaw – Интернет-право, киберправо # законы, относящиеся к Интернету и компьютерным правонарушениям (*computer offense*), в том числе к нарушениям авторского права (*copyright infringement*) и различным видам мошенничества (*fraud*) (см. также *cybercrime*).

cyber operation – кибероперация # в кибервойне (см. также *cyberwarfare*).

cyber penetration – кибервзлом, кибератака – см. *cyber attack*.

cyber protection – киберзащита, защита от киберугроз # например, cyber protection capability – возможности киберзащиты (см. также *cybersecurity, cyber threat*).

cyber resilience – устойчивость к киберугрозам (кибератакам), киберустойчивость # см. также *cybersecurity, cyber threat*.

cyber risk – киберугроза, риск (угроза) кибербезопасности (компьютерной безопасности, ИБ) # пример: No country, industry, community or individual is immune to cyber risks. – Никто сейчас не застрахован (не защищён) от киберугроз – ни государство, ни индустрия, ни общество, ни личность (см. также *cybersecurity, cyber threat*).

cybersecurity (*также* **cyber security**, **cyberspace security**) – безопасность в киберпространстве, кибербезопасность (КБ), Интернет-безопасность # комплекс технических, технологических, инфраструктурных и законодательных мер, процессов и практик, обеспечивающих эффективное обнаружение кибератак (*cyber attack*) и противодействие им, то есть защиту киберпространства (компьютерных сетей, устройств, программ и данных) от подобных атак. Кибербезопасность является составной частью Интернет-безопасности. Требует подготовки соответствующих специалистов-профессионалов; в современных условиях всепроникающей компьютеризации приобретает всё более важное значение для государства, промышленности, общества и каждого человека. Современный кибертерроризм является составной частью гибридных войн и одним из действенных рычагов достижения политических целей на международной арене. Особенностью кибертерроризма является стремление атакующих сделать совершённый террористический акт не только имеющим опасные последствия, но широко известным населению, чтобы он получил большой общественный резонанс. Например, cybersecurity risk management – управление рисками в области кибербезопасности (ИБ); cyber security expert – эксперт по кибербезопасности. Синоним – *information technology security* (см. также *airport cybersecurity, cyberdefense, cyber incident, cyber potential, cyber protection, cyber risk, cybersecurity analyst, cybersecurity application, cybersecurity certificate, cybersecurity employer, cybersecurity expert, cybersecurity infrastructure, cybersecurity market*, *cybersecurity report, cybersecurity technology, cyber threat, information security*, *Internet security, malicious circuit, security, security operations center, threat intelligence*).

cybersecurity adviser – советник по кибербезопасности (КБ) # должность в ряде правительственных организаций США (см. также *cybersecurity*).

cybersecurity analyst – аналитик по вопросам кибербезопасности (КБ) # специальность в организациях, занимающихся ИБ (см. также *cybersecurity, cybersecurity researcher*).

cybersecurity application – приложение для кибербезопасности (КБ) # см. также *application, cybersecurity*.

cybersecurity business – бизнес в области кибербезопасности (КБ) # см. также *cybersecurity*.

cybersecurity certificate – сертификат (аттестат, диплом) специалиста по кибербезопасности (КБ) – см. *cybersecurity*.

cybersecurity employer – работодатель для специалистов по кибербезопасности (КБ) – см. *cybersecurity*.

cybersecurity expert – эксперт по (в области) кибербезопасности (КБ) # см. также *cybersecurity*.

cybersecurity hardening (*также* **hardening**) – повышение уровня ИБ, уровня кибербезопасности (КБ), устойчивости, робастности системы # в ИБ – достигается, в частности, путём составления, измерения, анализа и сокращения поверхности атаки и поверхности уязвимостей системы. Для ПО это выявление и удаление необязательных функций, кодов, логинов, сервисов – векторов атаки. В компьютерных системах обычно предусматривается создание многоуровневой защиты – с применением средств противодействия вредоносному ПО (*malware*), с регулярной диагностикой средств безопасности и регулярным обновлением ПО при помощи “заплаток” от изготовителей, с удалением ненужных приложений, с физической изоляцией от небезопасных сетей и др. (см. также *air gap, antispyware, antivirus, attack, attack surface, cybersecurity hardening guide, defense in depth*, *information security, robustness, security diagnosis, vulnerability, vulnerability surface*).

cybersecurity hardening guide – руководство по повышению кибербезопасности (КБ) – см. *cybersecurity hardening*.

cybersecurity incident (*также* **cyber security incident**) – нарушение кибербезопасности (КБ), киберинцидент; инцидент в области кибербезопасности – см. *cyber incident*.

cybersecurity infrastructure – инфраструктура кибербезопасности (КБ), инфраструктура КБ # см. также *cybersecurity, infrastructure.*

cybersecurity market (*также* **cyber security market**) – рынок средств кибербезопасности, рынок КБ # этот рынок включает такие средства и решения, как управление инцидентами нарушения безопасности (security incident management); Единая система защиты от угроз, мультифункциональные защитные устройства (Unified Threat Management, *UTM*); управление рисками и контроль соответствия руководящим документам (risk and compliance management) и Система идентификации и управления доступом (Identity and Access Management, IdM, IAM). Этот комплекс решений позволяет организациям обезопасить свою инфраструктуру и данные от вредоносных киберугроз и уязвимостей (см. также *cybersecurity, security, security incident, threat, vulnerability*).

cybersecurity report – сообщение о нарушении кибербезопасности (КБ), отчёт о компьютерной безопасности # см. также *cybersecurity*.

cybersecurity researcher – исследователь[, работающий] в области кибербезопасности (КБ) # см. также *cybersecurity analyst*.

cybersecurity solution (*также* **cyber security solution**) – решение в области кибербезопасности (КБ) – см. *security solution*.

cybersecurity spending – расходы на кибербезопасность # см. также *cybersecurity, IT security investment*.

cybersecurity strategy – стратегия [обеспечения] кибербезопасности (КБ) # это может быть как предмет обсуждений и исследований, так и основная функция, ответственность группы, работающей в компании по данному направлению (см. также *cybersecurity, strategy*).

cybersecurity technology – технология кибербезопасности (КБ) – см. *cybersecurity*.

cybershenanigans – махинации с использованием сетевых компьютеров, кибермахинации # см. также *cybercrime*.

cybersleuth – кибердетектив, киберсыщик # см. также *cybercrime*.

data breach – утечка данных; уязвимость данных; несанкционированный доступ к данным # одна из главных проблем ИБ, чреватая большим материальным ущербом и риском других потерь. Для предотвращения этих потерь принимаются самые разные способы защиты – аппаратные, программные, организационные и др. Например, average cost of a data breach – средняя стоимость утечки данных (средняя величина ущерба, потерь от инцидента утечки данных) (см. также *data breach notification, data security, malicious breach*).

data leakage – утечка данных # воровство корпоративных данных злоумышленниками в результате несанкционированного доступа или нелояльными служащими, инсайдерами, производимое с различными целями (для продажи, компрометации данных и др.) (см. также *data leak prevention, data security, data theft, leakage, loss of data*).

data privacy – конфиденциальность (приватность) данных # в ИБ – требует специальных мер по защите данных от несанкционированного доступа (НСД), неавторизованных изменений и др. (см. также *confidentiality, data privacy policy, data privacy regulations, data protection, security*).

data security – защита (защищённость, безопасность) данных # защита данных от неавторизованного (случайного или преднамеренного) раскрытия, модификации или разрушения; обеспечение конфиденциальности, целостности и доступности данных (информации). Достигается применением аппаратных, программных и криптографических методов и средств защиты, а также комплексом организационных мероприятий. Например, industry data security standard – отраслевой стандарт по безопасности данных (см. также *confidentiality, corporate data security, data breach, data control, data leakage, data modification, data protection, data room, file encryption, information security, security*).

defense in depth (*также* **defense-in-depth**, **defence in depth**) – многоуровневая защита [системы, сети, организации] # стратегия обеспечения ИБ с использованием человеческого фактора, технологических и операционных методов и средств – создание нескольких уровней (слоёв, барьеров) средств и способов обеспечения защиты системы (компьютера, приложения) и/или организации (см. также *antivirus, hardening*, *information security, vulnerability*).

destruction – уничтожение, разрушение # в ИБ и криптографии – процесс перезаписи, стирания или физического разрушения информации (например, цифровых, электронных секретных данных, криптографических ключей, учётных данных и др.) таким образом, чтобы её невозможно было восстановить и использовать. Синонимы – demolition, *disintegration* (см. также *data destruction, deletion, wipe, zeroization*).

disclose information – разглашать информацию # см. также *disclosure*.

disclosure – демаскирование, раскрытие; разглашение; открытие; разоблачение; обнаружение # в ИБ – information disclosure (disclosure of information, divulge information) – раскрытие или разглашение секретной (конфиденциальной, корпоративной и др.) информации лицам, доступ которым к ней запрещён (см. также *inadvertent disclosure, nondisclosure agreement, security, STRIDE, unauthorized disclosure, vulnerability disclosure*).

DMZ – demilitarized zone – демилитаризованная зона # часть компьютерной сети, находящаяся логически между локальной сетью и Интернетом. Обеспечивает выход в Интернет и присутствие в нём, скрывая при этом внутреннюю сеть организации и предотвращая прямое обращение к ней, т. е. защищая от внешних атак соответственно принятой политике безопасности (см. также *attack, firewall, IDS, LAN, security, security perimeter*).

downgrade (*также* **downgrading**) – 1. понижение уровня, категории (качества, секретности, защищённости, ответственности, прав доступа и др.) # в ИБ – авторизованное снижение степени защищённости конкретной секретной информации, например перевод информации и/или компьютерной системы с умеренного (*moderate impact*) на низкий (*low impact*) уровень риска, уязвимости (см. также *classified information, declassification, downgraded, high impact, impact, security, vulnerability*); 2. понижение (в звании, должности, статусе, оценке и т. п.).

DPaaS – Data Protection as a Service, Data Protection-as-a-Service – защита данных (ЗД) как услуга (как сервис), модель (технология) обеспечения сохранности данных DPaaS # см. также *BURR, data protection, service.*

DSO – Data Security Officer – ответственный за безопасность данных # сотрудник, отвечающий за обеспечение безопасности обработки данных в системе и за противодействие попыткам несанкционированного к ним доступа и их использования (см. также *data security, security, security administrator, security audit, security management*).

eavesdropping – перехват, прослушка, прослушивание [передач, данных, сообщений] # перехват данных, пересылаемых по линии связи, например содержимого незащищённых транзакций. Различают пассивный перехват (passive eavesdropping) – перехват без воздействия на обмен сообщениями, и активный (*active eavesdropping, active wiretap*), когда атакующий не просто контролирует обмен, но и изменяет передаваемые и/или добавляет свои сообщения (см. также *eavesdropping attack, eavesdropping device, interception, listening, man-in-the-middle attack, security, sniffer, tap*).

eavesdropping attack – атака подслушиванием # вид атаки, в которой атакующий вначале пассивно прослушивает обмен данными по протоколу аутентификации, чтобы собрать информацию, которую потом можно использовать для активной атаки, представляясь легальным претендентом на установление соединения (см. также *active attack, claimant, eavesdropping*, *passive attack*).

electronic warfare (**EW**) – электронная война, война с применением электронного оружия; радиоэлектронная война, радиоэлектронная борьба (РЭБ) # радиоэлектронное подавление;

противодействие радиоэлектронному подавлению со стороны противника; использование электронных устройств, работающих в электромагнитном спектре, или направленной [электромагнитной] энергии для нарушения работоспособности, вывода из строя или разрушения компьютерных и телекоммуникационных систем и ВЦ противника. Электронная война может вестись пилотными и беспилотными системами вооружения с воздуха, моря, земли, космоса, причём её целями могут быть людские ресурсы, коммуникационные системы, радиолокационные средства и/или другие виды оборудования и систем противника. Пример: Electronic warfare specialists are called “crows” because commanders referred to them by the code name “Raven” during World War II. – Специалистов по радиоэлектронной войне называют “в***о***ронами”, потому что во время Второй мировой войны командование вызывало их по кодовому слову “Ворон” (см. также *information warfare*).

encrypted software – ПО с криптографической защитой # применяется для обеспечения информационной безопасности в военных, финансовых, государственных и иных ответственных, критически важных системах (*mission critical systems*).

enterprise security – корпоративная безопасность; политика и служба безопасности корпорации (организации) # в ИБ – методы и средства, решения и сервисы, обеспечивающие кибербезопасность (КБ) бизнеса, предприятия, организации, то есть защиту центров обработки данных (ЦОД), физических оконечных систем, мобильных устройств, электронной почты, других коммуникационных каналов от зловредного ПО и кибератак (см. также *cybersecurity, security*).

entrapment – подставка (*разг.* подстава); ловушка # в ИБ – провокация киберпреступления с целью его изобличения или преднамеренное внесение явных дефектов в компьютерную систему или в криптографическое оборудование с целью своевременного обнаружения попыток вредоносного проникновения (атаки) или взлома системы в процессе эксплуатации (см. также *trap*).

evidence – 1. доказательство, вещественное доказательство (вещдок); основание; свидетельство; подтверждение; улика # в ИБ – вещественное доказательство (вещдок), на основании которого можно, например, определить причину инцидента. Например, compelling evidence – убедительное доказательство (см. также *body of evidence, chain of evidence, digital evidence, exculpatory evidence, incident*, *inculpatory evidence*, *objective evidence, security*);
2. служить доказательством, доказывать; подтверждать # см. также *tamper evidence*.

exculpatory evidence – доказательство (доказательства) невиновности # в ИБ – исключение вины, в данном случае той или иной причины ИБ-инцидента (киберинцидента), в результате рассмотрения и анализа имеющихся вещественных

доказательств (вещдоков) (см. также *evidence, examination, incident, inculpatory evidence*, *security*).

external security testing – внешнее тестирование средств обеспечения безопасности # тестирование средств обеспечения безопасности (средств информационной защиты), которое производится из-за границ информационной среды организации, из-за периметра безопасности (см. также *security perimeter, security testing*).

false negative (**FN**) – ошибочный отказ [в доступе к системе]; ложно отрицательная [аутентификация, идентификация] # в ИБ – ситуация, когда зарегистрированный (легальный) пользователь пытается пройти идентификацию по биометрическим атрибутам (например, по отпечаткам пальцев), но из-за ненадёжной работы средств контроля получает отказ (*ср. false positive*; см. также *authentication, biometric identification, false-negative result, FAR, identification system*).

false positive (**FP**) – 1. ошибочный допуск [к системе]; ложно положительная [аутентификация, идентификация] # в ИБ – ситуация, когда средства биометрической аутентификации (биометрические, двухфакторные или иные) идентифицируют атакующего, злоумышленника или просто случайного человека как зарегистрированного пользователя и ошибочно разрешают ему доступ к ресурсам и данным компьютерной системы и сети, что является серьёзным нарушением информационной безопасности (ср. *false negative*; см. также *authentication, biometric identification, FAR, identification system*);
2. ложно положительный # ошибочный результат работы программы (приложения, системы), воспринимаемый как правильный. Например, false positive alerts – ложные положительные предупреждения (см. также *false-positive result*).

file protection – защита файла (файлов) # в ИБ – совокупность процессов и процедур, призванных предотвращать несанкционированный доступ, заражение (инфицирование), удаление, модификацию или разрушение файла или каких-либо частей его контента; обеспечивается на уровне ОС путём разделения (разграничения) прав доступа (см. также *file, file security*).

file sandboxing – проверка файла (файлов) в песочнице # в ИБ – анализ поведения неизвестных (подозрительных) файлов с соблюдением максимальных мер безопасности, в изолированной защищённой среде (см. также *sandbox*).

file security – безопасность файлов # в ИБ – меры и средства, благодаря которым доступ к компьютерным файлам предоставляется только авторизованным пользователям (см. также *file protection*).

FIRST – Forum for (of) Incident and Response Security Team – Форум команд по ИБ и реакциям на инциденты ИБ, форум FIRST # всемирный форум, объединяющий все группы реагирования на нарушения информационной безопасности (*CERT*), которых в 2014 г. насчитывалось 304, а также занимающийся их сертификацией и определяющий правила, которые они должны соблюдать (см. также *CSIRT, incident, incident response, security, www.first.org*).

foothold expansion – *букв.* расширение плацдарма; упрочение позиции атакующего # в ИБ – создание атакующим дополнительных лазеек, которые используются для повторных (многократных) проникновений в систему или сеть после первоначальной инфильтрации в неё вредоносного ПО (см. также *attack, back door, infiltration, malware, threat actor*).

fraud – 1. обман, мошенничество, жульничество # пример: "The laws allow the use of monitoring where fraud or crime is suspected" (T. Shimomura). – Законодательство разрешает использовать мониторинг в случаях, когда подозревается мошенничество или преступление (Ц. Симомура). Синоним – *scam* (см. также *adfraud, click fraud, computer fraud, consumer fraud protection, FPF, fraud detection, fraudulent, identity fraud, online fraud*); 2. фрод # мошенничество с пластиковыми (банковскими, дебетовыми, кредитными) карточками и др. (см. также *bankcard fraud, debit card fraud, financial security, plastic card, skimming*).

GDPR (*также* **EU GDPR**) – General Data Protection Regulation – Общие правила защиты данных, регламент Евросоюза GDPR; закон о защите персональных данных, закон GDPR # правила защиты персональных данных (ПД), вступившие в действие 25 мая 2018 года, предусматривают жёсткие требования по сбору, хранению, передаче и любой обработке ПД всех граждан и резидентов Евросоюза и Европейской экономической зоны (ЕЭЗ, European Economic Area, EEA) и жёсткие санкции за их несоблюдение. Организации обязаны внедрить средства контроля ПД на уровне отдельных пользователей, обезличивать эти данные и удалять их по запросу соответствующего лица, вести отчётность по соблюдению этих и других требований (см. также *data protection, personal data, privacy*).

grey hat hacker – серый хакер # в хакерском сообществе так называют квалифицированного хакера, который берётся за любую работу и занимает промежуточное положение где-то между белыми и чёрными хакерами (см. также *hacker, hacking, hacking community*).

greylist (*также* **graylist**, **gray list**, **grey list**) – серый список # записи в базе данных, перечисляющие все устройства, смарт-карты и иные объекты, которые находятся под подозрением в отношении безопасности (см. также *blacklisting, greylisting, hotlist, whitelist*).

greyware (*также* **grayware**) – “серое” ПО # *1*. общий термин, употребляемый иногда для обозначения приложений, которые ведут себя раздражающе или нежелательно, но при этом менее опасны и серьёзны по своим последствиям, чем вредоносное ПО; *2*. вредоносные программы (*malware*), попадающие в “серую зону” между обычным ПО и вирусами. К этой категории относятся такие опасные и/или надоедливые программы, как *adware, spyware, trackware* и многие другие.

guard code – защитный код, код безопасности # *1*. секретный пароль пользователя для разблокировки телефона/смартфона; *2*. защитный код кредитной или дебетовой банковской карточки (трёхзначное или четырёхзначное число), используется обычно для обеспечения безопасности покупок через Интернет; *3*. программа-аутентификатор, проверяющая при входе в систему личность пользователя и его права доступа. Частичный синоним – *security code* (см. также *authenticator, guard, password*).

hacker – хакер # в программистском сообществе, где возник этот термин (*MIT*, конец 1950-х годов), означал лицо (специалиста), пользующееся своими глубокими знаниями определённых систем и процессов для выявления в них уязвимостей и для достижения “нестандартных” целей. Среди молодых людей того времени существовала даже определённая хакерская культура, базирующаяся на принципах открытого обмена программами и приёмами конструирования аппаратуры между друзьями. Не случайно одним из истинных, белых хакеров, сообщающих разработчикам и владельцам систем об обнаруженных уязвимостях, был Ричард Столман (Richard Stallman), написавший редактор EMACS, а затем основавший *FSF,* а также Линус Торвальдс (Linus Torvalds), разработчик ОС Linux. Слово hacker возникло, скорее всего, от hack through – “прорубиться”. Позже, после выхода в 1983 г. фильма War Games, это слово стало ассоциироваться со словом “*cracker*” и людьми, злонамеренно взламывающими программы и проникающими в чужие компьютеры, к защищённым ресурсам, – зловредными хакерами (*malicious hacker*), серыми или чёрными хакерами (dark-side hacker). Отметим, что буквальный перевод *black hat hacker* – хакер в чёрной шляпе и *white hat hacker* – хакер в белой шляпе; эти термины появились по ассоциации с чёрно-белыми голливудскими вестернами, где в чёрных шляпах были плохие, а в белых – хорошие парни (см. также *criminal hacker, ethical hacker, grey hat hacker, hackathon, hacker attack, hackerese, hacker group, hacker threat, hacking, hacking community, intruder, phreaker, script kiddie, security*).

hacker attack (*также* **hack attack**) – атака хакеров, хакерская атака – см. *attack*.

hacker group – хакерская группа # неформальное объединение хакеров. Пример: Every minute of every day there are governments, organized crime, and hacker groups turning the doors on your house looking for an unlocked entry. – Ежедневно и ежеминутно государственные службы, организованные преступные группировки и хакерские группы

ищут лазейки и пытаются проникнуть в ваш дом (в вашу систему) (см. также *back door, hacker*).

hacker-powered security (*также* **hacker-powered security program**) – обеспечение безопасности благодаря белым хакерам, программа обеспечения безопасности с участием белых хакеров # в ИБ США – программа привлечения белых (этических) хакеров для выявления уязвимостей (*vulnerability disclosure*) компьютерных систем; сейчас становится практически обязательной нормой для самых различных организаций, от Фейсбука (*Facebook*) до государственных учреждений. Так, ведущие компании США, причём не только технологические, выплачивают хакерам до 1 млн долларов в год в виде премий (*bug bounty*) за помощь в обнаружении уязвимостей и повышении безопасности своих компьютерных систем (сетей) и бизнес-приложений (см. также *ethical hacker, security, vulnerability*).

hacker threat – хакерская угроза # угроза безопасности компьютерной системе со стороны хакера (хакеров) (см. также *threat*).

hacking – 1. неавторизованный доступ [к компьютерным данным], проникновение [в систему], взлом программ, *разг.* хакерство # один из рисков ИБ – требует разнообразных мер защиты и обеспечения безопасности систем и данных (см. также *attack, cybersecurity risks, data security, hacker, hacking spike, hacking techniques, hacking tool, threat*);
2. *проф.* хакинг, хакерство # у истинных хакеров – процесс проникновения в суть той или иной вещи для понимания того, "как это работает". Результатом такого этичного, или белого, хакинга может быть критика реализации системы, алгоритма и т. п. и предложения по устранению уязвимостей, нахождение максимально эффективного или элегантного решения задачи. Злонамеренный, или деструктивный, хакинг (*destructive hacking*) обычно направлен на хищение значимой информации, получение контроля над компьютером для включения его в зомби-сеть (*botnet*) и т. п. Пример: Among people who write code, though, the term hack refers to a "quick-and-dirty" solution to a problem, or a clever way to get something done. – Однако среди программистов термин *hack* обычно означает решение проблемы "на скорую руку" или искусный способ быстро добиться нужного результата (см. также *ethical hacking, hacking community, hardware hacking*).

hacking community (*также* **hack community**) – сообщество хакеров, хакерское сообщество # неформальное сообщество программистов и любителей, занимающихся хакерской деятельностью (см. также *hacker, hacking*).

hacking spike – всплеск хакерской активности # см. также *hacker*.

hacking techniques – методы (приёмы) хакинга – см. *hacking.*

hacking tool – инструмент неавторизованного доступа (хакинга) # см. также *hacking*.

hardware security – 1. аппаратная защита # механические, электромеханические, электронные, оптические, лазерные, радиотехнические и другие устройства, используемые в компьютерных сетях и системах для защиты данных от несанкционированного доступа (см. также *security*);
2. безопасность аппаратных средств.

hardware vulnerability – аппаратная уязвимость, уязвимость аппаратного обеспечения # синоним – *hardware weakness* (см. также *hardware, information security, vulnerability*).

hardware weakness – аппаратная уязвимость # уязвимость компьютерной или сетевой системы, связанная с её аппаратным обеспечением. К таким уязвимостям, относятся, в частности аппаратные закладки. Синоним – *hardware vulnerability*.

high impact (**HI**, **HIM**, **HIMP**) – сильное воздействие, сильный эффект; высокая уязвимость, высокий риск, большой ущерб # в ИБ – потеря или нарушение конфиденциальности (*confidentiality*), целостности (*integrity*) или готовности (*availability*), в результате чего можно ожидать серьёзных или катастрофических последствий для работы организаций, для активов организаций, для физических лиц, для национальных интересов страны. Это может быть резкое снижение функциональных возможностей организации, уменьшение активов, большие финансовые убытки, тяжкие телесные повреждения или смерть людей (см. также *impact, high-impact system, security*).

high-impact system – система высокой уязвимости # в ИБ – компьютерная система, для которой как минимум один из базовых целевых показателей безопасности (конфиденциальность, целостность или готовность) имеет высокую потенциальную возможность (высокий риск) нарушения (см. также *high impact, security*).

high-tech crime (*также* **high tech crime**, **hi-tech crime**) – высокотехнологичное преступление; высокотехнологичная преступность # категория преступлений, связанных, в частности, с современными информационными технологиями, особенно с Интернетом, – это, например, распространение разнообразных вирусов, хакерские атаки, направленные на незаконное получение конфиденциальной, в том числе финансовой, информации, дезорганизацию работы банков, корпораций, государственных учреждений и т. п. Синонимы – *computer crime, cybercrime, electronic crime*, *e-crime* (см. также *INTERPOL*).

honeynet – сеть-приманка, сеть-ловушка # реальная или виртуальная сеть из хостов-приманок (см. также *honeypot*).

honeypot – хост-приманка, хост-ловушка # изолированный от внутренней сети хост, специально подготовленный для атак взломщиков. На таких приманках-ловушках с незакрытыми известными уязвимостями ловятся атакующие, изучаются их поведение, применяемые ими методы и инструменты (см. также *cracker, honeynet*).

human factor (**HF**) – человеческий фактор # самое слабое звено в компьютерной (и не только компьютерной) безопасности. Пример: “Only two things are infinite, the universe and human stupidity, and I’m not sure about the former” (Albert Einstein). – Бесконечны только две вещи: вселенная и человеческая глупость, при этом у меня нет полной уверенности лишь относительно первой из них (Альберт Эйнштейн). Синоним – human element (см. также *human involvement, peopleware*, *social engineering, wetware*).

hybrid security control – гибридный контроль безопасности; гибридное управление безопасностью # в ИБ – политика безопасности систем организации, сочетающая в себе черты общего управления безопасностью и специфичных для системы средств защиты (безопасности) (см. также *common control, computer security, security control, system-specific security control*).

ICSA – International Computer Security Association – Международная ассоциация по компьютерной безопасности # начала свою деятельность в 1992 году под названием *NCSA*. В тестированиях, проводимых ICSA Labs, используется вредоносный код как из собственной “коллекции”, так и из списка *WildList*. По результатам исследований продуктам выдаётся сертификат ICSA – его удостаиваются те антивирусы, которые способны обнаружить 100% вирусов из списка *WildList*, выпущенного за месяц до испытаний, и не менее 90% вирусов из собственной коллекции ICSA (см. также *CheckMark, ITW, VB100%*).

identity, credential, and access management (**ICAM**) – система идентификации, электронных удостоверений (ЭУ) и контроля доступа ICAM # в ИБ – государственная система США, призванная предотвращать несанкционированный доступ (НСД) к критически важным ресурсам, данным, компьютерным информационным системам (ИС) и другим подобным объектам (см. также *access management, attribute-based access control, credential, identity, security*).

identity theft (*также* **electronic identity theft**) – хищение личных (конфиденциальных) данных [о человеке], *досл.* “кража личности” # в информационной безопасности – вид компьютерного мошенничества, когда злоумышленник (или вредоносная программа) при осуществлении криминального действия выдаёт себя за другого человека. К этой категории относятся, например, хищение номеров кредитных карточек или захват аккаунтов пользователей. Например, identity theft protection – защита от кражи личных

данных. Синоним – *identity fraud* (см. также *account hijacking, after-theft diagnosis, computer crime, security*).

impact – 1. воздействие, влияние, эффект # например, impact of cyberthreats on your business – влияние киберугроз на ваш бизнес;
2. (*также* **impact level**) – [негативные] последствия; потенциальный ущерб # в ИБ – величина потенциального ущерба (вреда) для организации в результате несанкционированного раскрытия, модификации или разрушения информации, либо потери информации или вывода из строя информационных систем (см. также *high impact, impact analysis, impact value, low impact, moderate impact, potential impact, security*);
3. оказывать воздействие.

impact value – величина потенциального ущерба # в ИБ – оценочная величина потенциального ущерба (вреда) для организации вследствие нарушения конфиденциальности, целостности или готовности информационной системы (ИС) и её информации; эта величина может быть низкой, средней или высокой – и она определяет соответствующую степень (категорию) безопасности ИС (low, moderate, high) (см. также *availability, confidentiality, impact, integrity, security*).

impersonation (*также* **impersonating**) – имперсонация; *не реком*. олицетворение # маскировка нарушителя (злоумышленника) или вредоносной программы под законного пользователя или легальную программу; например, by impersonating a legitimate diagnostic tool – подделываясь (маскируясь) под легальное средство диагностики. Разновидность спуфинга (*spoofing*) (см. также *verifier impersonation attack, eavesdropping, masquerading, security*).

inadvertent disclosure – непреднамеренное раскрытие информации # в ИБ – вид инцидента, когда информация случайно раскрывается лицу, не имеющему допуска на доступ к этой информации (см. также *incident, security, unauthorized disclosure*).

incident – 1. происшествие, событие, эпизод # см. также *accident*;
2. инцидент, неприятное происшествие, столкновение;
3. инцидент # в ИБ – ситуация в компьютерной системе, связанная с зафиксированным несанкционированным доступом или его попыткой, атакой или взломом. Нарушение или неминуемая угроза нарушения принятых политик безопасности или стандартных рекомендованных практик обеспечения безопасности компьютерных систем. Событие, которое реально или потенциально ставит под угрозу конфиденциальность, целостность или готовность таких систем либо данные, которые они обрабатывают, хранят или передают. Более строго, инцидент определяется как актуализация риска – событие или результат реализации угрозы, связанной с уязвимостью системы. Синоним – *cyber incident* (см.

также *event, incident handling, incident modeling, incident response plan, security incident, vul nerability*);
4. непредвиденный (случайный) отказ техники; нештатная ситуация # см. также *disaster recovery*;
5. особая ситуация или ошибка, требующая проведения расследования # любое событие в работе программы или системы, требующее исследования и анализа. Синоним – *deviation* (см. также *anomaly, incident diary*).

incident diary – дневник (журнал) [учёта] инцидентов [ИБ] # предлагается пользователям системы для фиксации встретившихся им проблем, способов их разрешения (если удалось это сделать) и оценки сложности проблем, например по шкале Лайкерта (*Likert scale*). Ведение подобных журналов (в электронном виде) способствует повышению надёжности и удобства эксплуатации систем (см. также *diary, incident*).

incident handling – обработка инцидента (инцидентов) [ИБ] # в ИБ – методы и средства смягчения вредных последствий при нарушениях политик и рекомендованных практик обеспечения безопасности компьютерных систем. Например, incident handling team – группа обработки инцидентов (см. также *incident, incident reporting, incident response plan, security incident*).

incident management – контроль происшествий (инцидентов) [ИБ] # одна из подсистем в системах сетевого управления (см. также *incident scope, incident response, network management*).

incident outsourcing – инцидентный аутсорсинг # модификация аутсорсинга – привлечение внешних подрядчиков-соисполнителей для решения конкретных проблем по запросам заказчика; бывает более эффективным и экономически оправданным, чем обычный (постоянный) аутсорсинг (см. также *incident, insourcing, outsourcing*).

incident prevention – предупреждение инцидентов [ИБ] # см. также *incident*.

incident reporting – отчётность по инцидентам [ИБ] # в зависимости о уровня серьёзности инцидента, отчётность по нему может быть либо обязательной, либо необязательной (см. также *incident, incident handling, mandatory reporting*).

incident response – реакция на инцидент [ИБ] # например, incident response procedure – процедура реакции на инцидент; incident response policies – политики реакции на инциденты (см. также *incident*, *incident diary, incident response plan*).

incident response plan – план реагирования на инциденты [ИБ] # в ИБ – заранее определённый документированный набор инструкций или процедур, направленных на

обнаружение и обработку инцидентов, ограничение и смягчение последствий вредоносных кибератак на компьютерные системы организации (см. также *incident handling, security*).

incident scope – масштаб инцидента [ИБ], “масштаб бедствия” # в ИБ – размеры повреждений и потерь в результате вредоносной атаки на компьютерные системы организации, количество (объём) украденных данных, величина и характеристики поверхности атаки (*attack surface*), а также стоимость устранения последствий данной атаки (to resolve the attack) и мер по предотвращению подобных успешных атак в будущем (см. также *attack, incident, incident management, security*).

incident solving (*также* **incident resolving**) – разрешение инцидента (инцидентов ИБ) # в ИБ – диагностика, выявление и устранение причин инцидента, предотвращение или уменьшение его неблагоприятных последствий, ущерба, вреда для системы, организации (см. также *incident, incident handling, security*).

inculpatory evidence – доказательство (доказательства) виновности, улики; вещественные доказательства # в ИБ – вещественные доказательства (вещдоки), позволяющие прогнозировать увеличение вероятности нарушения защиты программной системы или возникновение инцидента (инцидентов) (см. также *exculpatory evidence, evidence, examination, incident*, *security*).

intruder – взламыватель, злоумышленник, нарушитель, атакующий # неавторизованный, обычно злонамеренный (malicious intruder), пользователь (или программа), пытающийся получить несанкционированный доступ (НСД) в компьютерную систему. Потенциальные злоумышленники называются источниками угрозы (*threat source*) (см. также *computer security, cracker, hacker threat, interloper, IP spoofing, malicious actor, security, snooper, target software, trespasser*).

intruder detection – обнаружение нарушителей, выявление нарушителей # совокупность мер, способов, специализированного ПО и устройств для определения присутствия в сети или попыток входа в сеть неавторизованных пользователей – как физических лиц, так и программных средств (см. также *attack detection, IDS, intruder, security*).

intrusion – вторжение, [насильственное] проникновение, появление без приглашения; вмешательство # в ИБ – несанкционированное проникновение в систему в обход её защитных механизмов (см. также *attack, computer security, IDS, information security, intrusion prevention, intrusion senso r, intrusion tool, session hijacking*).

intrusion attempt – попытка проникновения [в систему/сеть] # см. также *attack*.

intrusion detection – обнаружение проникновения (вторжения) – см. *intrusion*.

intrusion prevention – предотвращение вторжений # технологии, позволяющие обнаруживать и устранять уязвимости (слабые места) системы до того, как они будут использованы для её взлома. Для этого прежде всего производится мониторинг трафика по таким протоколам, как *HTTP*, *SNMP*, *TCP/IP*. Например, network intrusion prevention system – система предотвращения сетевых вторжений (атак) (см. также *attack detection, intruder detection, IPS, network security*).

intrusion prevention system (**IPS**) – система предотвращения вторжений, СПВ # система блокирования несанкционированных действий, попыток атаки в момент их появления и нарушения информационной безопасности; система мониторинга сетевого трафика и обнаружения вторжений на основе поведения. Такие системы интегрируются с другими средствами защиты: с антивирусным ПО, межсетевыми экранами (*firewall*), сканерами безопасности (*security scanner*), системами управления инцидентами и т. п. Являются развитием систем *IDS* (см. также *HIDS, network IPS device, network security, NIDS, security breach*).

intrusion sensor – датчик охранной сигнализации # элемент системы безопасности жилых и производственных помещений. Синоним – intrusion detector (см. также *intrusion detection*).

intrusion testing – тестирование [системы] на вторжение (проникновение) # см. также *ethical hacking, penetration testing*.

intrusion tool – средство вторжения, инструмент для проникновения (атаки) # см. также *intrusion*.

IOC – indicator of compromise – признак компрометации, признак вторжения (проникновения) [в систему, сеть] # в ИБ – признаки (индикаторы, вещественные доказательства, улики и т. п.), которые можно найти после вредоносного вторжения в систему (сеть) и по которым специалисты могут что-то понять относительно вида атаки или наличия бреши (уязвимости) в средствах защиты и безопасности системы. Такими признаками могут быть IP-адреса, имена доменов, хэш-коды (хэш-значения) вредоносных файлов, сигнатуры вирусов и другие подобные артефакты (см. также *compromise*, *investigator*).

IT-related risk – риск, связанный с ИТ; ИТ-риск # в ИБ – вероятность того, что из-за конкретного источника угрозы и конкретной уязвимости одной или нескольких корпоративных систем будет нанесён серьёзный ущерб организации или бизнесу. В качестве примеров факторов риска можно назвать неавторизованное (злонамеренное,

незлонамеренное или случайное) раскрытие, модификацию или разрушение информации; совершённые без злого умысла ошибки и упущения при создании и эксплуатации ИТ-систем; выход из строя ИТ-ресурсов в результате стихийных бедствий или антропогенных (техногенных) катастроф и др. (см. также *security*).

IT security architecture – архитектура [обеспечения] безопасности ИТ-систем # описание принципов обеспечения безопасности и общего подхода к реализации этих принципов при разработке систем; например, рекомендации по размещению и внедрению специальных сервисов безопасности в различные распределённые вычислительные среды (см. также *security*).

IT security awareness – информирование по проблемам ИТ-безопасности; осведомлённость в проблемах ИТ-безопасности – см. *awareness*.

IT security education – образование по ИТ-безопасности, образование в области ИБ # преподавание студентам профильных специальностей и специалистам математических и технических дисциплин, имеющих отношение к вопросам обеспечения безопасности (см. также *information security education, IT security awareness, IT security training, security*).

IT security investment – инвестиции в ИТ-безопасность # затраты на специалистов по ИТ/ИБ, обучение персонала, приобретение и внедрение ИТ-приложений или систем, предназначенных исключительно для обеспечения информационной безопасности и др.; например, закупка системы обнаружения вторжений (*IDS*) и инфраструктуры *PKI* (см. также *cybersecurity spending, security*).

IT security threat[s] – угроза (угрозы) безопасности ИТ-систем # в ИБ – требуют выявления, анализа и оценки для принятия адекватных мер защиты и предотвращения возможных неблагоприятных последствий (см. также *attack, cyber threat, information security*, *security threat, vulnerability*).

IT security training – обучение по ИТ-безопасности # рассчитано на сотрудников организации, не являющихся специалистами по ИТ-безопасности (на управленческий персонал, разработчиков систем, снабженцев, аудиторов и др.); цель – дать им необходимый минимум знаний и умений для выполнения конкретных функций (см. также *IT security awareness, IT security education, IT security skills, security*).

Kerberos ticket – билет Kerberos, мандат Kerberos # в ИБ – средство управления доступом, в частности для доменов безопасности *Windows* (см. также *security, security domain*).

key management – управление [криптографическими] ключами # общий термин, обозначающий все административные функции по генерации, распределению

(распространению), сохранению, обновлению, уничтожению и адресации криптографических ключей и других данных, связанных с ИБ (например, паролей), на протяжении всего жизненного цикла ключей (см. также *cryptographic key*, *FIREFLY*, *key*, *key management device, key management infrastructure, password*).

KRB – см. *Kerberos*.

labeled security protection – защита по меткам безопасности # механизм контроля доступа к системе, в котором решение о предоставлении доступа к тем или иным ресурсам принимается с учётом их меток безопасности (см. также *access control, security label*).

laboratory attack – лабораторная атака # в ИБ – восстановление (чтение) информации носителя данных в лабораторных условиях при помощи сложного современного оборудования (см. также *attack*).

layered defense – эшелонированная оборона # в ИБ – многоуровневая архитектурная организация средств защиты компьютерной системы (сети), существенно повышающая их эффективность и реальное обеспечение безопасности. Синонимы – defense in depth, multilevel defense, *multilevel security* (см. также *safety, security*).

leakage – утечка [данных, информации] # несанкционированное и/или злоумышленное чтение, копирование, искажение или уничтожение конфиденциальной информации; например, копирование данных в незащищённое приложение с более низким уровнем безопасности, чем требуется с точки зрения секретности информации, на мобильные носители (компакт-диски, дискеты, USB-накопители), печать, открытие, редактирование чужих документов и т. д. Существует много способов и путей (каналов) утечки информации. Частичный синоним – *spillage* (см. также *anti-leakage software, data breach, data leakage, leak, leakage channel, leakage path*).

leakage channel – канал утечки [данных] # см. также *leakage, leakage path*.

least privilege (*также* **least privilege principle**, **principle of least privilege**, **PoLP**) – принцип минимума прав доступа (привилегий); принцип минимально необходимых прав доступа # в ИБ – способ ограничения доступа к информационным ресурсам для процессов, по аналогии с принципом *need-to-know* для пользователей; предоставление пользователям только тех прав доступа и только к тем ресурсам, которые необходимы им для выполнения служебных обязанностей. Принцип разработки такой архитектуры ИБ, которая предоставляла бы каждому объекту лишь минимально необходимые для выполнения его функций системные ресурсы и права доступа к ним (см. также *clearance*, *mandatory access control, security*).

logical perimeter – логический периметр # в ИБ – концептуальный периметр, охватывающий всех потенциальных пользователей системы, которые подключены к ней прямо или опосредованно и получают выходные данные системы без надёжного контроля со стороны соответствующей полномочной организации (см. также *boundary, boundary protection, perimeter defense, physical perimeter, security perimeter*).

loss of data (*также* **data loss**) – потеря данных # *1*. возможные последствия сбоев-отказов системы, выхода из строя оборудования, ненадёжности устройств памяти, действий злоумышленного, вредоносного ПО и т. п.; *2*. один из рисков ИБ – раскрытие корпоративной, проприетарной или секретной информации в результате хищения или утечки данных (см. также *backup, cybersecurity risks, data destruction, data leakage, data loss, data loss prevention, data security, loss prevention, loss-sensitive traffic, security*).

loss prevention – предотвращение потерь # в компьютерной безопасности – совокупность мер, предотвращающих вывод корпоративной сети из строя и потерю ценной информации.

low-impact system – система невысокой (малой, низкой) уязвимости # в ИБ – компьютерная система, для которой все три базовых целевых показателя безопасности (конфиденциальность, целостность или готовность) имеют низкую потенциальную возможность (низкий риск) нарушения (см. также *low impact, security*).

malicious – злонамеренный; злоумышленный; зловредный, вредоносный # например, malicious weapons – вредоносное оружие. Синонимы – spiteful, malign, hurtful (см. также *malicious act, malicious activity, malicious applets, malicious attack*, *malicious circuit*, *malicious code, malicious email, malicious item, malicious website*).

malicious act – злоумышленное (вредоносное) действие (деяние); деяние, совершённое со злым умыслом # см. также *malicious activity, malicious code, malicious hacker*.

malicious activity – вредоносная (злонамеренная) деятельность # см. также *malicious act*.

malicious actor – злоумышленник, нарушитель # синонимы и частичные синонимы – *attacker, cracker,* deliberate criminal, evil-doer, *impostor, intruder*, malefactor, *malicious hacker, malicious user, manipulator, plotter, snooper, threat actor*, *trespasser*, *violator* (см. также *actor*).

malicious applets – вредоносные аплеты # небольшие прикладные программы, которые автоматически скачиваются из Сети и запускаются, причём выполняя неавторизованные функции (операции) в приложениях (см. также *applet, malware*).

malicious attack – злонамеренная атака, вредоносная атака # см. также *malicious software, malware attack*.

malicious behavior – злоумышленное (вредоносное) поведение # один из признаков вредоносного ПО (см. также *malicious activity, malware*).

malicious circuit – вредоносная микросхема # микросхема, содержащая аппаратную закладку или недокументированную возможность, которые могут быть использованы для получения несанкционированного доступа к системе, для вывода системы из строя или перехвата
данных. Пример: Hidden malicious circuits provide an attacker with a stealthy attack vector. – Схемы со скрытыми вредоносными "закладками" представляют собой тайный вектор атаки для злоумышленника (см. также *attack vector, cybersecurity, maliciously modified device*).

malicious code (**malcode**) – вредоносный код, вредоносная программа # например, malicious code attack – атака вредоносной программы. Синоним – *malicious software* (см. также *file-based attack, malware*).

malicious email – вредоносное электронное письмо, заражённое письмо # письмо с заражённым вложением, со ссылками на заражённый сайт, фишинговое письмо и т. д. (см. также *malicious code, malicious website*).

malicious hacker – злонамеренный хакер, зловредный хакер # синонимы – *black hat hacker, criminal hacker,* dark-side hacker, malicious code attacker (см. также *hacker, malicious act, malicious user*).

malicious item – вредоносный объект (элемент, файл, пакет, вирус, сообщение) # вредоносные или потенциально вредоносные (подозрительные) объекты должны обнаруживаться специальными антивирусными программами, изолироваться (помещаться в карантин) – чтобы они не могли причинить вред компьютеру, системе (см. также *anti-virus software, item, malicious, quarantine*).

malicious logic – вредоносная логика # аппаратные, аппаратно-программные или программные средства, которые скрытно и намеренно включены или введены в систему с вредоносными целями (см. также *malicious circuit, malware*).

maliciously modified device – злонамеренно модифицированное устройство # устройство, в котором установлены вредоносные микросхемы (см. также *malicious circuit*).

malicious software – вредоносное ПО – см. *malware*.

malicious tools – вредоносные утилиты, вредоносные инструментальные программы # программы, предназначенные для автоматизации создания вирусов, червей или троянских программ, DoS-атак на удалённые серверы, взлома других компьютеров и т. п. В отличие от вирусов, червей и троянских программ, вредоносные утилиты сами не представляют угрозы для компьютера, на котором исполняются, а вредоносные действия выполняются приложением только по прямому указанию злоумышленника (см. также *DoS, malware*).

malicious user – злонамеренный пользователь, вредоносный пользователь # см. также *malicious actor, malicious hacker*.

malicious website – вредоносный вебсайт # вебсайт, посещение которого может привести к заражению компьютера пользователя вредоносными программами. Посещение таких сайтов блокируется некоторыми антивирусами (см. также *antivirus protection, compromised website, malware*).

malvertising (*также* **malicious advertising**) – вредоносная реклама # использование онлайновой рекламы (*online advertising*) для распространения вредоносного ПО, с минимальным участием или без участия пользователей (см. также *malware*).

malware – *от* malicious software – вредоносные (злонамеренные) программы, *разг.* мэлвер # любая программа, скрытно введённая в компьютерную систему с намерением нарушить конфиденциальность, целостность или готовность её данных, приложений, ОС, т. е. действующая против интересов пользователя или владельца системы. К этой категории относятся все виды вирусов, черви, троянцы, шпионящее ПО, мэлвер для мобильных устройств (особенно для смартфонов) и т. п. Например, malware infection – заражение (инфицирование) вредоносным ПО. Синонимы – bad software, *harmful program, malevolent program, malicious code* (см. также *anti-malware, antivirus software, attack, botnet malware, cryptocurrency malware, disinfection, exploit, ICS targeting malware, infected machine, MaaS, malicious applets, malicious behavior, malicious file, malicious logic, malicious tools, malvertising, malware analysis, malware attack, malware detection, malware inspection, malware protection, malware robots, malware scanning, malvertising, password-stealing malware, PUM, smart-phone malware, threat, virus, web robot, zero-day threat detection*).

malware analysis – анализ вредоносного ПО # бывает статическим и динамическим (static and dynamic malware analysis) (см. также *malware, malware inspection, malware research*).

malware analyst – аналитик вредоносного ПО # должность в компаниях, занимающихся проблемами ИБ (см. также *malware, malware analysis*).

malware attack – атака [с использованием, с помощью] вредоносного ПО # один из серьёзных рисков кибербезопасности (КБ) – вредоносные действия инфицировавшего систему ПО, о котором владелец системы не знает (см. также *attack, cybersecurity risks, data security, malicious attack, malware*).

malware detection – обнаружение (выявление) вредоносного ПО # например, adversarial attacks against malware detection – состязательные атаки на средства обнаружения вредоносных программ (см. также *malware, malware inspection*).

malware-fighting engine (*также* **malware engine**) – движок борьбы с вредоносными программами (зловредами) # см. также *malware, malware detection*.

malicious file – файл с вредоносным ПО, заражённый файл # см. также *malware*.

malware forms of spyware – вредоносные виды шпионского (шпионящего) ПО # см. также *anti-spyware, malware, non-malware forms of spyware, spyware.*

malware inspection – проверка на наличие вредоносного ПО, проверка на мэлвер # многие поставщики брандмауэров (МЭ) заимствуют для этой цели традиционный метод антивирусной защиты настольных ПК: буферизуют загружаемые файлы, а потом проверяют их на наличие мэлвера. Такой подход не только вносит большие задержки, но и чреват рисками в отношении безопасности, поскольку объём имеющейся временной памяти может ограничивать максимальный размер файлов (см. также *firewall, malware, network security, security risk*).

malware protection – защита от вредоносного ПО (от мэлвера) # см. также *malware attack, malware detection, malware research, malware scanning engine*.

malware research – исследование вредоносного ПО (мэлвера) # исследование вредоносных программ для изучения используемых ими методов и создания средств противодействия им (см. также *malware analysis, malware protection, research*).

malware robots – вредоносные роботы # общее название программных веб-роботов, используемых злоумышленниками для неблаговидных, мошеннических, противоправных, преступных действий, афер, махинаций (см. также *malware, web robot*).

malware scanning – сканирование (поиск, обнаружение) вредоносного ПО # например, malware scanning technology – технология сканирования (поиска, обнаружения) вредоносного ПО (см. также *malware scanning engine, scanning*).

malware scanning engine – механизм сканирования (поиска, обнаружения) вредоносного ПО (мэлвера) # см. также *malware inspection, malware protection, scanning*.

malware stealing (*также* **malware cryptocurrency stealing**) – кража криптовалюты при помощи мэлвера # кража секретных ключей от криптокошельков с целью последующей кражи самой криптовалюты из этих кошельков (см. также *cryptocurrency malware, malware*).

man-in-the-browser attack (*также* **man in the browser attack**) – атака [злоумышленника] через браузер – см. *man-in-the-middle attack*.

man-in-the-middle attack (*также* **man in the middle**, **MITM**, **man in the middle attack**, **MITM attack**, **MitM attack**) – атака злоумышленника в роли посредника, атака типа MITM, MITM-атака # в криптографии и ИБ – разновидность активного перехвата сообщений (см. *eavesdropping*), когда атакующий устанавливает независимые соединения со своими жертвами-абонентами, которым кажется, что они общаются между собой по частной линии связи, в то время как фактически их разговор (обмен сообщениями) проходит под контролем атакующего; при этом атакующий каждому абоненту выдаёт себя за его собеседника (благодаря подложной взаимной аутентификации) и может даже вставлять в разговор свои сообщения. Большинство криптографических протоколов (*cryptographic protocol*) содержат средства предотвращения MITM-атак. В Интернете и в системах сотовой связи используются такие подкатегории подобных атак, как *man-in-the-browser attack* и *man-in-the-mobile attack,* для защиты от которых требуются новые средства. Синоним – *bucket brigade attack* (см. также *ARP spoofing, attack*, *cybersecurity, masquerade*, *mutual authentication, replay attack, security*).

man-in-the-mobile attack (*также* **man in the mobile attack**) – атака [злоумышленника] через мобильный телефон – см. *man-in-the-middle attack*.

manipulative communications deception (**MCD**) – манипуляционная дезинформация при коммуникациях # в ИБ – изменение передаваемых сообщений или симуляция дружественных телекоммуникаций с целью дезинформации, дезориентации противника. Один из способов радиоэлектронной борьбы, РЭБ (см. также *communications cover, communications deception, imitative communications deception, manipulation, security*).

moderate impact (**MI**, **MIM**, **MIMP**) – *букв.* умеренное воздействие, умеренный эффект; умеренная (средняя) уязвимость, умеренный риск, умеренный ущерб # в ИБ – потеря или нарушение конфиденциальности (*confidentiality*), целостности (*integrity*) или готовности (*availability*), в результате чего можно ожидать не слишком серьёзных последствий для работы организаций, для активов организаций, для физических лиц, для национальных

интересов страны. Это может быть снижение функциональных возможностей и эффективности работы организации, заметное уменьшение активов, значительные финансовые убытки, телесные повреждения, но не смерть людей (см. также *impact, moderate-impact system, security*).

moderate-impact system – система умеренной уязвимости # в ИБ – компьютерная система, для которой как минимум один из базовых целевых показателей безопасности (конфиденциальность, целостность или готовность) имеет умеренную потенциальную возможность (умеренный риск) нарушения, но ни один из них не имеет высокого риска нарушения (см. также *moderate impact, security*).

National Vulnerability Database (**NVD**) – Национальная база данных уязвимостей, репозиторий стандартов NVD (США) # государственный репозиторий США, который хранит данные по управлению уязвимостями, собираемые при помощи протокола *SCAP*. Эти данные позволяют автоматизировать управление уязвимостями, измерение параметров безопасности, контроль соблюдения требований регуляторных органов, спецификаций и др. NVD содержит контрольные списки для оценки средств безопасности; сведения об известных ошибках ПО, влияющих на безопасность; варианты неправильных, рискованных конфигураций; списки применяемых продуктов; количественные показатели потенциального ущерба при разных атаках и др. (см. также *impact, security, vulnerability*).

need-to-know (*также* **need-to-know principle**) – тем, кому положено знать, для узкого круга лиц; для служебного пользования (ДСП) # в ИБ – принцип минимума необходимой информации; разговорный термин для обозначения сравнительно низкого уровня допуска к секретной работе и/или секретным материалам. Метод ограничения доступа к информационным ресурсам – пользователю предоставляется доступ только к той информации, которую ему необходимо знать для выполнения своей работы, но не более; это также принцип минимума прав доступа, привилегий (*least privilege*). При этом принцип need-to-know обычно действует для людей, а least privilege – для процессов (см. также *clearance*, *mandatory access control, need-to-know determination, security*).

need-to-know determination (*также* **need to know determination**) – определение минимума необходимой информации # в ИБ – авторизованный держатель секретной информации решает, какому пользователю он может предоставить доступ к ней для выполнения официальных обязанностей этого пользователя (см. также *clearance, least privilege, need-to-know, security*).

network-based attack – сетевая атака, атака сетевого уровня # в ИБ – атака, проводимая со стороны компьютерной сети и использующая особенности функционирования сетей,

уязвимости в различных сетевых протоколах и службах. Для защиты от таких атак широко применяются межсетевые экраны, антивирусы и др. средства (см. также *DDoS*).

obfuscation – запутывание [программного кода], *проф.* обфускация # (*от лат.* obfuscare – затенять, затемнять; и *брит.* obfuscate – делать неочевидным, запутанным, сбивать с толку) в ИБ – приведение исходного текста или исполнимого кода программы (при его генерации) к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и возможность модификации с использованием декомпиляции; иногда делается для уменьшения объёма кода. Такая технология реализуется, в частности, в крипторах (*crypter*). Синонимы – *metamorphing, mutation* (см. также *executable code, obfuscator*, *security*).

off-line attack (*также* **offline attack**) – офлайновая атака, офлайн-атака # атака, в которой злоумышленник вначале добывает необходимые ему данные (обычно путём перехвата сообщений протокола аутентификации или путём проникновения в систему и кражи секретных файлов), после чего анализирует их при помощи системы по собственному выбору (см. также *attack, off-line, online attack*).

online attack (*также* **on-line attack**) – онлайновая атака, онлайн-атака # атака компьютерную систему, корпоративную сеть, веб-сайт и др., проводимая через Интернет, например атака на протокол аутентификации с целью получить как бы легальный доступ к системе или узнать секретные данные для аутентификации. Пример: It is often difficult to locate the source of an online attack. – Источник (инициатора) онлайновой атаки зачастую очень трудно локализовать (установить) (см. также *attack, off-line attack, verifier impersonation attack*).

operational vulnerability information – оперативная информация по уязвимости # в ИБ – информация, описывающая присутствие уязвимости в конкретной операционной среде или сети (см. также *vulnerability*).

outside threat (*также* **outsider threat**) – внешняя угроза # в ИБ – угроза от неавторизованного субъекта или объекта, находящегося за пределами (границами) домена безопасности и имеющего потенциальные возможности нанести вред корпоративной системе путём разрушения, раскрытия и/или модификации данных и/или вывода системы из строя. Синонимы – *external threat,* outer threat (см. также *inside threat*).

passive attack – пассивная атака, пассивное нападение # в компьютерной безопасности – нападение на систему или на сеть, которое трудно обнаружить, когда, например, злоумышленник подключается к каналам передачи данных и прослушивает сеть, чтобы определять характеристики передаваемых данных, читать и анализировать сообщения, не

изменяя их и не меняя режимы работы. Синоним – *passive assault* (см. также *attack, eavesdropping, sniffing*).

passive hiding – пассивное сокрытие [информации] # в ИБ – способ технической защиты информации путём ослабления энергетических характеристик физических сигналов, полей или уменьшения концентрации веществ (см. также *active hiding, security activity*).

password (**PSWD**, **PW**) – пароль # код (секретная уникальная последовательность символов – букв, цифр и/или специальных знаков), необходимый пользователю для аутентификации, проверки идентичности и для получения доступа к закрытой (защищённой) системе, системным ресурсам или сервису. Например, encrypted blockchain password – зашифрованный пароль доступа к блокчейну. Синонимы – *code word*, countersign, *parole, watchword* (см. также *access code, authentication password, BIOS password, blockchain password*, *boot-up password*, *brute-force attack, character-based password, cleartext password, insecure password, login, logon password, network password, one-time password, passcode, passphrase*, *password aging, password attack, password cracker, password equivalence, password fishing, password generator, password guessing, password management, password protection, password verification, picture password, PIN, plain-text password, salt, weak password*).

password cracking – взлом паролей # процесс получения (восстановления, распознавания, угадывания, определения, похищения) секретных паролей, хранящихся в компьютерной системе или передаваемых по сети (см. также *password cracker*).

password protection – 1. защита паролём, *проф.* защита паролём, защита с помощью (с использованием) паролей, парольная защита # в ИБ – использование паролей в качестве средства, позволяющего получить доступ к компьютерной системе, системным ресурсам и данным только авторизованным пользователям. Пример: Password protection against illegal copying is not effective. – Защита паролём неэффективна против (от) нелегального копирования [ПО]. Частичный синоним – *password protected* (см. также *password, protection, security*);
2. защита паролей # в различных системах ИБ значение термина может существенно варьироваться – от шифрования паролей до их периодической замены. Синоним – *password security* (см. также *password aging*).

penetration testing (*также* **pentest**, **pentesting**, **penetration test**, **pen testing**) – испытание проникновением, *проф.* пентест # в ИБ – поиск уязвимостей и оценки безопасности компьютерной системы, веб-приложения, сети или хоста с помощью взлома, проводимый с разрешения владельца. Во время такого тестирования тестировщик, используя всю имеющуюся документацию (по архитектуре и реализации системы, по исходным текстам, по эксплуатации), устраивает псевдоатаку на корпоративную систему

или компьютерную сеть, инсценируя (имитируя) действия реальных злоумышленников, или атаку, проводимую каким-либо вредоносным ПО без непосредственного участия самого взломщика. Испытания проникновением существенно различаются по способу их организации. Существуют стандартизированные методологии проведения пентестов (GWAPT, IEM, OWASP). Итогом испытаний является письменный отчёт с перечислением обнаруженных уязвимостей, уровня риска, связанного с каждой из них, и рекомендациями по снижению рисков. Такое тестирование должно проводиться периодически, поскольку изменения конфигурации сети, установка новых приложений и т. п. могут вызвать появление новых уязвимостей. Синонимы – *ethical hacking*, white-hat hacking; частичный синоним – *intrusion testing* (см. также *exploit, penetration tester, pentesting toolkit, security, targeted testing, testing, vulnerability level*).

perimeter defense – защита периметра [безопасности системы, сети, организации]; защита по периметру # по аналогии с круговой обороной в военном деле – осуществляется с помощью сетевых экранов, антивирусных сканеров, систем обнаружения атак и др. (см. также *air gap, firewall, IDS, logical perimeter*, *security perimeter, security solution, virus scanner*).

potential impact – потенциальный ущерб, потенциальный вред # в ИБ – потеря (нарушение) конфиденциальности, целостности или готовности (доступности) компьютерных систем, в результате чего можно ожидать ограниченных (низких, малых), серьёзных (умеренных, средних) или катастрофических (высоких, сильных) вредных последствий для бизнеса организации, её активов или для людей (см. также *availability, confidentiality, high impact, impact analysis, impact value, integrity, low impact, moderate impact, security*).

quarantine – 1. карантин; карантинизация; изоляция # исходно медицинский термин, означающий размещение заражённых (больных) людей или зверей отдельно от здоровых, чтобы минимизировать опасность эпидемии, широкого распространения инфекционного заболевания; в ИБ – изолирование подозрительных файлов, предположительно содержащих мэлвер, вредоносные программы, для будущего исследования или "дезинфекции", обеззараживания. Находящиеся в карантине файлы не будут исполняться, однако пользователь может восстановить их, если окажется, что подозрения были неоправданными (см. также *disinfection, infection, malware, sandbox, security*); 2. изолировать.

red team – "красная команда", независимая группа специалистов-аудиторов (аналитиков) # в США такие группы привлекаются (часто секретно) для анализа деятельности гражданских и военных организаций с целью повышения их эффективности, исследования и прогнозирования возможных сценариев развития событий в мировой экономике и военных конфликтах. Аналогичные группы высококвалифицированных

специалистов по информационной безопасности (ИБ) проводят тестирование систем (сетей, приложений) для выявления уязвимостей и др. (см. также *ethical hacking*, *intelligence community, red teaming, security, vulnerability scan*).

remediation plan – план устранения уязвимостей или угроз # в ИБ – план по устранению одной или нескольких угроз или уязвимостей, обнаруженных при аудите безопасности (защищённости) корпоративных систем организации; в этом плане обычно указываются возможные способы устранения угроз или уязвимостей и приоритетность выполнения работ (см. также *remediation, threat, vulnerability*).

replay attack – атака путём повтора (с использованием) перехваченных данных # в ИБ – ситуация, когда атакующий перехватывает передаваемую по каналам связи информацию аутентификации или информацию управления доступом, затем ретранслирует её с целью получения несанкционированного доступа (НСД) к системе. Пример: Some cryptographic protocols are vulnerable to replay attacks. – Некоторые криптографические протоколы уязвимы к атакам путём повтора перехваченных данных (см. также *attack, nonce*, *unauthorized access*).

replay attack detection (*также* **replay detection**) – обнаружение атаки, проводимой путём повтора (с использованием) перехваченных данных # в ИБ, в стандарте *IPSec*, в протоколах *TKIP* и *CCMP* (см. также *replay attack*).

rule-based security policy – политика безопасности на основе правил # в ИБ – политика безопасности, предусматривающая для всех субъектов установление глобальных правил, согласно которым обычно производится сравнение чувствительности (важности, секретности, уязвимости, *sensitivity*) объектов доступа и соответствующих атрибутов (прав, привилегий) субъектов, запрашивающих доступ к этим объектам. Частичный синоним – *discretionary access control* (см. также *access control*, *security policy*).

rules of engagement (**ROE**) – правила совместной работы # в ИБ – детальные руководящие указания и ограничения, касающиеся проведения тестирования средств безопасности корпоративной информационной системы (КИС). Эти правила утверждаются до начала тестирования и предоставляют команде специалистов-тестировщиков права выполнять все оговорённые действия без дополнительных разрешений (см. также *rule, security testing*).

secret – 1. (*также* **secrecy**) – секрет, тайна # сведения, данные, информация, документы, критически важные для страны, организации, человека, не подлежащие разглашению, широкому распространению, охраняемые и защищаемые различными государственными законами, корпоративными положениями и др. Соответственно различают государственную, служебную, коммерческую, технологическую, врачебную

тайну, персональные данные (ПД), конфиденциальные сведения разной степени секретности и др. (см. также *classified secret, manufacturing secret, private data, state secret, technological secret, trade secret*);
2. секретно (С) # гриф (форма допуска к секретным материалам и/или к секретной работе) (см. также *classification, confidential, security clearance, top secret*);
3. секретный, тайный # см. также *secret communication, secret key, secret seed*.

secure web gateway (SWG) – защищённый веб-шлюз # программная система, обеспечивающая защиту от внешних веб-угроз (*web threat*) – вредоносного и шпионящего ПО, нежелательного веб-контента, фишинга и т. п. (см. также *attack, exploit, malware, threat, vulnerability*).

secure web service – защищённый веб-сервис # см. также *Web service*.

secure wireless network – защищённая беспроводная сеть # беспроводная сеть, оснащённая средствами защиты (например, криптографической) передаваемых данных (см. также *wireless network*).

secure zone – зона безопасности – см. *chained secure zone*.

securing – обеспечение безопасности, организация защиты # например, securing computer-based resources – обеспечение безопасности компьютерных ресурсов (см. также *resecuring, security*).

security – 1. защита; защищённость, безопасность # общий термин, охватывающий методы, средства и технологии физической, информационной и иных видов защиты от атак, угроз и рисков для объектов, систем, сетей, предприятий, пользователей и др.; в частности, свойства ПО и аппаратного обеспечения, обеспечивающие предотвращение несанкционированного доступа (случайного или намеренного) к программам и данным (см. также *A1 security, access control, attack, authorization, communication security, computer security, content security software, crimeware, cryptographic security, data security, emission security, information security, Internet security, login security, network security, physical security, proactive security, security administrator, security agent security architecture, security audit, security breach, security certification, security context, security design, security engineering, security erase, security evaluation, security hole, security kernel, security log, security management, security model, security patch, security perimeter, security policy, security protocol, security scanner, security service, security solution, security technology, security testing, security textbook, security threat, security tools, security vulnerability, traffic-flow security, transmission security, Web security*);
2. служба безопасности # см. также *security audit, security certification, security management, security policy, wireless security*;

3. секретность, конфиденциальность, защищённость # пример: “Neither the first Ethernet local area network nor the first Internet computer networks were built with privacy or security in mind” (T. Shimomura). – При разработке как первой локальной сети Ethernet, так и первых компьютерных сетей Интернета о проблемах защищённости персональных данных и безопасности практически не думали.

security activity – активность защиты [информации] # в ИБ – принцип защиты, предусматривающий целенаправленное навязывание противнику (например, техническим разведкам противника) ложного представления об объекте защиты в соответствии с замыслом (стратегией) защиты, а также противодействие средствам технической разведки. Упреждающее предотвращение (нейтрализация) угроз ИБ (см. также *security, security threat*).

security administrator (**security admin**, **secadmin**) – администратор [системы] безопасности # специалист, обслуживающий средства защиты корпоративной сети; готовит и устанавливает политики ИБ; проводит оценку защищённости корпоративный ИТ-ресурсов, а также занимается устранением угроз ИБ. Пример: Root and administrative level passwords are the keys to the kingdom for an intruder. – Пароли корневого и административного уровня открывают злоумышленнику доступ к системе (сети) (см. также *CSO, DSO*$_{[2]}$*, network security, system administrator*).

security advice – рекомендации по обеспечению безопасности, рекомендации по ИБ # см. также *cybersecurity, safety, security.*

security analysis – анализ надёжности (защищённости, безопасности) # в частности, анализ решения по ИБ. Пример: A complex system can also mean an increased difficulty for security analysis and secure implementation, a poorer performance, and a higher overhead cost for running and maintenance. – Сложность системы может также означать повышенную трудность анализа её надёжности и реализации требований безопасности, меньшую производительность и увеличенные накладные расходы при эксплуатации и техническом обслуживании (см. также *security*).

security analyst – аналитик в области безопасности # см. также *information security analyst, security analytics*.

security analytics – аналитика безопасности # обеспечивается специализированным ПО. Например, security analytics platform – платформа для аналитики безопасности (см. также *big data security analytics, information security, security analyst*).

security architecture – архитектура системы безопасности # например, security architecture solutions – решения в области архитектуры систем безопасности (см. также *security, X.800*).

security assessment – оценка (оценивание) качества обеспечения безопасности # пример: A security assessment can provide necessary information on how business processes use network technology. – Оценка качества обеспечения безопасности позволяет получить информацию, необходимую для определения эффективности использования сетевой технологии бизнес-процессами (см. также *security, security assessment report*).

security assessment report (**SAR**) – отчёт по оценке средств обеспечения безопасности # (*ранее* – certification package, пакет документов по сертификации) в ИБ и технологиях управления рисками – документирование детальных результатов тестирования, сертификации, аудита ИТ-систем по требованиям физической и/или информационной безопасности (см. также *safety, security, security assessment*).

security association – согласование мер безопасности, связь для обеспечения безопасности # в ИБ – отношения, устанавливаемые между двумя или более объектами (лицами, пользователями, организациями) с целью обеспечения защиты данных, которыми они обмениваются (см. также *security*).

security audit – проверка (контроль, аудит) [средств] защиты контроль средств безопасности # в ИБ – проверка функционирования систем защиты и работы персонала на соответствие требованиям безопасности с предупреждением сетевого администратора о выявленных нарушениях защиты. В более узком смысле – это выявление в результате бесед с руководителями предприятия (компании) и инструментальных проверок нарушений политик безопасности, надёжности организации защиты систем, организации регистрации, хранения и анализа данных, затрагивающих безопасность объекта оценки, реагирования на возможное нарушение безопасности, а также подготовленности персонала и физической безопасности и др. Пример: Firewalls and intrusion detection systems mean nothing if your passwords are compromised. – Брандмауэры (межсетевые экраны, МЭ) и системы обнаружения вторжений оказываются бесполезными, если вы не можете обеспечить секретность своих паролей (см. также *audit guide, network security, security administrator, security breach, security consulting*)

security awareness – осведомлённость [персонала] о правилах [информационной] безопасности # см. также *security*.

security banner – баннер секретности # размещаемый в верхней или нижней части компьютерного экрана баннер с общими указаниями, касающимися секретности системы. Этот термин обозначает также начальную заставку системы с информацией для

пользователей относительно правил ИБ, которые необходимо соблюдать при доступе к компьютерным ресурсам (см. также *banner, safeguarding statement, security*).

security best practices – лучшие практические методы по обеспечению безопасности, ИБ # см. также *best practice, cybersecurity, safety, security.*

security breach – нарушение защиты, взлом системы; брешь (нарушение) в системе безопасности # пример: Security breaches can cause malfunctions ranging from annoying to life-threatening. – Нарушения (бреши) в системе безопасности могут приводить к самым разным нежелательным последствиям, от раздражающих сообщений до угроз (риска) для жизни. Частичный синоним – computer breach (см. также *attack, breach, cracker, loophole, security audit, security penetration, vulnerability*).

security bug – ошибка, опасная для (с точки зрения) [компьютерной, информационной] безопасности. Синоним – *security error*.

security cable – трос (тросик) безопасности # средство защиты от воровства для мобильных и иных небольших, но дорогостоящих устройств, например мониторов, ноутбуков, компьютеров Mac Pro и др. – используется для прикрепления подобных устройств к стене, столу или другой тяжёлой или неподвижной конструкции при помощи специальных замков (см. также *kensington lock*).

security camera – камера видеонаблюдения # видеокамера, предназначенная для записи событий на объекте наблюдения с целью предупреждения преступлений и помощи в их раскрытии. Например, wireless security camera – беспроводная камера видеонаблюдения; Wi-Fi-connected security camera – камера видеонаблюдения с интерфейсом *Wi-Fi* (см. также *security, video camera, video surveillance*).

security categorization – категоризация (классификация) по секретности # в ИБ – процесс определения (установления) конкретной категории секретности и необходимой защищённости (и присвоения грифа секретности) для информации или информационной системы (ИС) по методологиям, регламентируемым специальными документами (см. также *category, security category, security classification*).

security category – категория секретности; степень, уровень секретности # в ИБ – уровень секретности и соответствующей защищённости, присваиваемый документу, файлу, записи или информационной системе (ИС) в зависимости от важности и ценности содержащейся в них информации, на основе оценки потенциального вреда, который потеря (нарушение) конфиденциальности, целостности или готовности подобной информации или ИС может нанести организации, её активам и операционной деятельности, или индивидуальным

пользователям (см. также *availability, confidentiality, impact, integrity, security categorization*, *security level*).

sensitivity – 1. чувствительность, уязвимость, секретность # в ИБ – характеристика ресурса, системы или данных, показывающая их значимость или важность и, соответственно, необходимость защиты (представляется соответствующей меткой, *security label*) (см. также *data classification*); 2. способность быстро реагировать.

SIEM – security information and event management – управление информацией безопасности и событиями безопасности, технология SIEM # общее обозначение категории программных продуктов и сервисов, реализующих управление информацией безопасности (security information management, SIM) и управление событиями (инцидентами) безопасности (security event management, SEM) – поэтому аббревиатуры SEM, SIM и SIEM иногда употребляются как синонимы (взаимозаменяемые). При этом SEM обычно представляет мониторинг событий безопасности в реальном времени, выявление их взаимосвязей и оповещение ответственных лиц, а SIM обеспечивает журналирование и долговременное хранение собираемых данных по безопасности, их анализ и составление соответствующих отчётов. Расширение функциональности и развитие сетевых технологий обусловливают и изменение требований по безопасности – например, для обеспечения безопасности речевых данных появилась технология vSIEM (voice security information and event management). В общем, технологии и системы SIEM служат основой центров обеспечения безопасности (ЦОБ), центров оперативного реагирования на инциденты ИБ, они призваны предоставлять руководителям и сотрудникам служб безопасности ту информацию, которая будет способствовать обнаружению уязвимостей, угроз и предотвращению инцидентов ИБ. В то же время наряду с SIEM появляются новые, более совершенные технологии мониторинга событий, связанных с информационной безопасностью (ИБ), контроля и анализа поведения не только пользователей, но и разных сущностей, процессов, трафиков, объектов, приложений – с целью выявления и прогнозирования ИБ-рисков (см. также *big data security analytics, incident response, information security, security, security operations center, UBA, UEBA*).

signature analysis – сигнатурный анализ, анализ сигнатур # базируется на совпадении фрагмента кода или последовательности сигналов с эталонным образцом; используется, в частности, для контроля работоспособности аппаратуры компьютера или для защиты от известных вирусов, от атак (вторжений) и др. (см. также *heuristic analysis, intrusion prevention system, network security, signature, signature-based scanning, signature-based tools, signature engine, virus signature*).

signature-based scanning – сканирование (проверка) [компьютера] на наличие вирусов с известными сигнатурами # один из способов обеспечения информационной безопасности – позволяет обнаружить и нейтрализовать (удалить) известные вирусы (см. также *signature analysis*).

social engineering – "социальная инженерия", социотехника # методы и тактика злонамеренного проникновения, при которой злоумышленник путём "уговоров" обманывает пользователей или администратора (например, представляясь новым сотрудником), входит таким образом в доверие и добивается значимой информации о компании и/или её компьютерных системах, чтобы получить несанкционированный доступ к сети. Обычно злоумышленники учитывают особенности человеческой природы, играют на жадности, тщеславии жертвы – или на желании оказать помощь ближнему. Пример: "For me it wasn't difficult becoming proficient in social engineering" (Kevin D. Mitnik). – Мне было несложно стать знатоком социальной инженерии (см. также *cracker, dumpster diving, human factor, human-factors engineering, impostor, information security, low-tech attack, phishing, wetware*).

spillage – 1. (*также* **data spillage**) – утечка [данных, информации] # в ИБ – инцидент, в результате которого секретная или контролируемая несекретная информация передаётся в компьютерную систему, не авторизованную (не аккредитованную) для работы с материалами такого уровня секретности, для их хранения и/или обработки. Частичный синоним – *leakage* (см. также *classified information spillage, CUI, incident, security*); 2. потери от утечки [данных, информации].

spyware – spy software – шпионящее ПО, *разг.* шпионское ПО # ПО, разновидность мэлвера (*malware*); предназначается для незаметной установки на компьютере в приложении с целью сбора информации о пользователях или организациях без их ведома, например путём слежения за действиями пользователя. Перехватывает его почтовую переписку, вводимую им информацию, пароли и команды и сообщает о них заинтересованном лицу (или организации). Такое ПО – большая угроза для государства, бизнеса и неприкосновенности частной жизни. В общем случае шпионящим ПО можно считать любое ПО, которое тайно использует подключение к Интернету для связи с внешним сервером и перехвата данных. Отметим, что различают также вредоносные и не вредоносные виды шпионящего ПО (*malware forms of spyware, non-malware forms of spyware*). Синоним – *scumware* (см. также *anti-spyware, keystroke logger, security, spyware blocker*).

supply chain attack – атака на логистическую цепочку # в ИБ – атака, позволяющая противнику-злоумышленнику использовать импланты или другие уязвимости, заложенные в систему до её установки, чтобы получать несанкционированный доступ (НСД) к данным и манипулировать продуктами и/или сервисами информационных

технологий (аппаратными и программными средствами, ОС, периферийными устройствами) в любой момент в течение их жизненного цикла (см. также *attack, implant, supply chain*, *vulnerability*).

tampering – 1. злонамеренное несанкционированное вмешательство в работу аппаратных или программных средств [компьютера]; взлом системы # внесение изменений в систему, в компоненты системы, их поведение или в данные. Например, data tampering – незаконное умышленное изменение, искажение или хищение данных; фальсификация данных (как хранящихся в БД, так и передаваемых по сетевым соединениям); document tampering – подделка документов (см. также *protector, security, STRIDE, tamper*); 2. несанкционированное копирование микросхем (см. также *anti-tampering techniques, reverse engineering, tamper-proof*).

tamper-proof – защищённый (с защитой) от злонамеренного (несанкционированного) вмешательства, от взлома, от воровства, от неумелого, небрежного обращения, от внесения неавторизованных изменений # пример: Slightly more formally, we can say that a smart card is a portable, tamper-proof computer with a programmable data store. – Несколько более формально можно сказать, что смарт-карта – это защищённый от злонамеренного вмешательства миниатюрный компьютер с программируемым хранением данных. Синоним – *tamper-resistant* (см. также *anti-tamper, protection against tampering, tamper, tampering, tamper resistance, tamper tolerant software*).

targeted attack – целевая атака, целенаправленная атака, *проф.* таргетированная атака # компьютерная атака, направленная на конкретного пользователя, небольшую группу пользователей, компанию, организацию или на целые отрасли промышленности. Основные цели подобных атак – взлом компьютерных систем и кража конфиденциальной информации, разрушение веб-серверов и других важных ресурсов, нарушение производственных или бизнес-процессов организации, деятельности государственного ведомства и т. п. Этот тип атак получает всё большее распространение. Точные цифры убытков от таких атак оценить трудно, но это уже сотни миллиардов долларов (порядка 600 млрд в 2017 г.). Частичный синоним – эффективная целенаправленная атака, комплексная целенаправленная угроза, APT-атака (см. *advanced persistent threat, APT*) (см. также *attack, IoT-targeted attack, targeted attack protection*).

technical security controls – технические средства [обеспечения] безопасности # в ИБ – средства защиты компьютерной системы (КС), которые реализуются и действуют в самой КС благодаря механизмам, содержащимся в её аппаратных, программных или аппаратно-программных компонентах (см. также *safeguard, security*, *security controls, technical security*).

threat – опасность, опасная ситуация, опасное событие, угроза [ИБ] # термин используется для обозначения как действий злоумышленников, так и рисков – потенциально возможных, злонамеренных или иных действий, которые могут нарушить информационную безопасность, нанести вред, например опасность преодоления защиты (угроза безопасности) компьютерной системы. Угрозы можно разделить на внутренние (inner threats) и внешние (outer threats). Согласно ISO/IEC 13335 угроза – потенциальная причина нежелательного инцидента. Чаще всего угроза является следствием наличия уязвимостей в защите компьютерных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в ПО). Синонимы – danger, peril, *hazard*, menace, risk (см. также *active threat, advanced persistent threat, blended threat, cyber threat, hacker threat, hacking, inside threat, internal threat, intruder, IT security threat, modem threat, network threat, outside threat, physical threat, potential threat, security threat, threat analysis, threat control, threat detection, threat event, threat landscape, threat modeling, threat monitoring, threat prevention, threat response, threat scenario, threat shifting, threat space, unstructured threat, web threat*).

threat actor – агент угрозы, источник угрозы [ИБ]; исполнитель угрозы; злоумышленник; вредоносный актор (агент); атакующий # человек, компьютер или организация, действия которых вызывают события или инциденты, приводящие или могущие привести к компрометации системы защиты и к нарушениям безопасности другой организации. Синоним – *malicious actor* (см. также *actor, security, security threat*).

threat analysis – анализ угроз [ИБ] # в ИБ – оценка типов, масштабов и природы событий или действий, которые могут привести к неблагоприятным последствиям; оценка степени угроз применительно к конкретным уязвимостям и вероятности их осуществления для конкретной системы в конкретном операционном окружении. Синоним – *threat assessment* (см. также *operating environment, security, threat, threat identification, threat modeling, threat probability*).

threat assessment – оценка угрозы (угроз) [ИБ] # в ИБ – формальное оценивание степени опасности конкретной угрозы для компьютерной системы (ИС) или организации и описание природы этой угрозы. Синоним – *threat analysis* (см. также *security, threat*).

threat control – контроль угроз (рисков); защита от угроз (рисков) [ИБ] # например, защита от угроз (рисков) беспроводной связи (*wireless threats*).

threat data – исходные (необработанные, сырые) данные по угрозе (угрозам) [ИБ] # данные, собранные по потенциальным угрозам (киберугрозам) средствами разведки и платформы *threat intelligence platform* (см.
также *intelligence, threat information, threat intelligence*).

threat detection – обнаружение угроз [ИБ] # например, AI threat detection – обнаружение угроз с помощью средств ИИ (см. также *behavioral threat detection, TDS, threat, zero-day threat detection*).

threat event – событие угрозы [ИБ]; опасное, угрожающее событие # в ИБ – событие или ситуация, чреватая нежелательными последствиями, потенциальным вредом для системы и/или организации (см. также *security, threat*).

threat identification – идентификация угрозы [ИБ] # в оценке рисков – процесс идентификации источников угроз (см. также *threat analysis, threat source*).

threat intelligence – 1. сведения об угрозах [ИБ]; 2. сбор данных об угрозах [ИБ] # см. также *threat analysis, threat source*.

threat landscape – ландшафт угроз # общая текущая ситуация, общая картина угроз ИБ (см. также *security, threat*).

threat modeling – моделирование угроз [ИБ] # в ИБ – предусматривает обычно компьютерный анализ и имитацию сетевых угроз и атак, вредоносных программ и инструментов, действий злоумышленников, а также уязвимостей системы, возможных схем и способов защиты, необходимых ресурсов и ПО для обеспечения безопасности. Существуют различные методологии моделирования угроз ИБ и ПО, предназначенное для этой цели (см. также *security requirements, threat analysis, threat model space*).

threat model space – пространство модели угроз [ИБ] # предмет и средство исследования алгоритмов машинного обучения (МО) и алгоритмов искусственного интеллекта (ИИ); позволяет анализировать и выбирать направления развития и реализации систем обеспечения безопасности, систем распознавания, систем технического зрения (СТЗ) и др. (см. также *threat modeling, threat space*).

threat monitoring – мониторинг угроз [ИБ] # в ИБ – анализ, оценивание и экспертиза результатов аудита и другой информации, собранной в целях выявления (обнаружения) в информационной системе (ИС) тех событий, которые могут быть связаны с нарушениями безопасности (см. также *assessment, security, threat analysis*).

threat prevention – предотвращение угроз (угрозы) [ИБ] # см. также *firewall, threat*.

threat probability (*также* **probability of threat**) – вероятность угрозы, вероятность осуществления угрозы [ИБ] # для оценки допустимо использовать трёхбалльную шкалу (низкая, средняя и высокая вероятность) (см. также *threat analysis*).

threat profile – профиль угрозы [ИБ] # профиль угрозы содержит информацию об угрозе, включающую в себя: название угрозы, её общее описание, источник угрозы (исходя из модели нарушителя), способ реализации, объект защиты (активы, на которые направлена угроза), последствия осуществления угрозы, предпосылки возникновения угрозы (уязвимости) и др. (см. также *threat*).

threat report – отчёт об угрозах [ИБ] # документ, публикуемый агентствами и компаниями, специализирующимися на ИБ. Содержит описание текущей ситуации в области ИБ, новых типов угроз и трендов, а также ~~содержит~~ рекомендации по борьбе с новыми киберугрозами (см. также *threat, threat research*).

threat research – исследование угроз [ИБ] # анализ реальных и потенциальных угроз (и рисков). Например, threat research team – группа по исследованию угроз ИБ (см. также *threat, threat report*).

threat response – реакция на угрозу [ИБ], защита от угроз [ИБ] # пример: Complex, heterogeneous IT environments make data protection and threat response very difficult. – В современных условиях, когда ИТ-системы становятся всё более сложными и разнородными, весьма затрудняется защита данных и защита от угроз ИБ (см. также *security*).

threat scenario – сценарий угроз [ИБ] # в ИБ – частично упорядоченная по времени совокупность отдельных угрожающих событий (*threat event*), связанных с конкретным источником угроз (*threat source*) или с несколькими источниками (см. также *security, threat*).

threat sensitive – чувствительный к угрозам, подверженный угрозам # см. также *security, threat*.

threat shifting – изменение угрозы, смещение угрозы [ИБ] # в ИБ – реакция злоумышленника, обнаружившего (натолкнувшегося на) средства защиты системы: он меняет некоторые параметры своей вредоносной атаки, чтобы обойти эти средства защиты (см. также *security, security controls, threat*).

threat source – источник угроз [ИБ] # в ИБ – план-схема и метод, нацеленные на сознательное использование уязвимости системы, или ситуация и метод, которые могут сделать это случайно, непреднамеренно. Синоним – threat agent (см. также *intruder, security, threat*).

threat space – пространство угроз [ИБ] # совокупность всех возможных угроз информационной безопасности (ИБ), включая угрозы [от] окружающей среды, вирусов,

Интернета и др. (см. также *information security, SWOT, threat model space, threat space search*).

threat space search (*также* **threat-space search**, **TSS**) – поиск (определение) пространства угроз (уязвимостей), поиск в пространстве угроз [ИБ] # одно из средств обеспечения информационной безопасности (ИБ) и защиты системы от злонамеренных атак, а в некоторых играх, например Го, – способ нахождения оптимальных решений (ходов), ведущих к выигрышу (см. также *threat space*).

threat window – окно опасностей, окно угроз [ИБ] # в ИБ – время с момента появления уязвимости до момента её устранения (это иногда часы, дни или более длительный период) – и обновления базы данных известных угроз, вирусов, атак с соответствующими сигнатурами, которая обычно используется средствами (механизмами) защиты и позволяет снизить вероятность взлома системы, защитить её от нового вида атаки. Если окно опасности открыто, злоумышленник может произвести успешную атаку на систему (см. также *attack, signature, security, threat, threat intelligence, virus, vulnerability*).

trusted computer system – доверенная компьютерная система, безопасная (защищённая) система # в ИБ – система, в которой реализован комплекс мер информационной и физической защиты согласно принятой политике обеспечения безопасности, что позволяет использовать её для одновременной обработки разной чувствительной (конфиденциальной) или секретной информации. Синоним – *protected computer system* (см. также *classified information, computer system, sensitive information, security*).

trusted path – доверенный тракт, доверенный канал [взаимодействия] # в ИБ – механизм, позволяющий пользователю или оператору (при помощи устройства ввода данных) непосредственно взаимодействовать (при соблюдении требований безопасности) с функциональными блоками защиты компьютерной системы или иного целевого объекта для поддержки принятой политики безопасности этой системы или объекта (см. также *information system, path, security, security policy, target of evaluation, trusted*).

unknown attack – атака неизвестного типа, неизвестная атака # в отличие от уже известных атак (known attack) (см. также *attack*).

untrusted – ненадёжный, непроверенный; не заслуживающий доверия; незащищённый, небезопасный # в ИБ – о процессе, приложении, компьютере, системе и др. Антоним – *trusted* (см. также *reliable, secure, security, untrusted process*).

untrusted process – непроверенный процесс # в ИБ – потенциально опасный процесс, который не прошёл проверку и оценку на корректность и соответствие требованиям

политики безопасности; он может содержать вредоносный код и попытаться обойти механизмы защиты системы (см. также *malicious code, security, security policy*).

user security function – механизм обеспечения ИБ (информационной безопасности) пользователя # реализует такие функции, как аутентификация, авторизация, сохранение конфиденциальности данных, целостности и доступности данных (см. также *information security*).

vaccine – "вакцина" # программа, обеспечивающая защиту против вирусов дополнительной проверкой целостности операционной системы. Синонимы – *antivirus software, virus protection software* (см. также *virus*).

virus (*также* **computer virus**) – [компьютерный] вирус # тип вредоносных программ, характеризующихся способностью скрытого от пользователя саморазмножения для поражения других программ, компьютеров или сетей. Под саморазмножением понимается способность вируса создавать собственную копию и внедрять её в тело заражаемого исполнимого файла, в документ, содержащий макрокоманды, в загрузочный сектор диска, почтовые сообщения и т. п. Таким образом, вирусы могут попадать в компьютер по электронной почте, через скачанные из Интернета программы, через заражённые съёмные носители и другими способами. Существует множество видов таких программ. Вирусы классифицируются по "среде обитания", способу заражения среды обитания, воздействию на компьютерную систему и особенностям алгоритма. По среде обитания вирусы делятся на загрузочные (*boot virus*), резидентные, файловые, дисковые, флэш-вирусы и сетевые. Термин предложил Фред Коэн (F. Kohen) в 1983 г., ещё когда он был студентом Университета Южной Калифорнии. Для борьбы с вирусами применяют антивирусные программы (*antivirus software*) (см. также *antivirus, antivirus virus, bacteria, cell-phone virus, content virus, cryptovirus, dropper, email virus, encrypted virus, file infector, ill-behaved software, infection, information warfare, logic bomb, macro virus, phage, polymorphic virus, slow infector, stealth virus, Trojan, vaccine, virus hoax, virus scanner, worm, Zoo virus*).

virus attack – вирусная атака # см. также *virus*.

virus code – [машинный] код вируса # чтобы затруднить разбор текстов вирусных программ, в них часто применяют самомодификацию и шифрование кода (см. также *self-encrypting virus, self-modifying code, virus*).

virus filtering – фильтрация вирусов, проверка на вирусы # контроль входящей и исходящей электронной почты, контента служб мгновенного обмена сообщениями (*instant messaging*) и/или загружаемых файлов на наличие компьютерных вирусов (см. также *virus protection, virus scanner*).

virus hoax (*также* **computer virus hoax**, **hoax**) – вирусный мистификатор # почтовое сообщение, которое не является вирусом, но указывает на якобы распространяющийся новый вирус и даёт рекомендацию, как его удалить с диска. Получателю рекомендуется разослать это письмо всем знакомым. Вирусный мистификатор может оказаться достаточно вредным, если указывает на важный системный файл (см. также *virus*).

virus infection – вирусная инфекция # заражение (инфицирование) компьютера вирусом (см. также *infection, virus*).

virus pattern – шаблон вируса # см. также *virus signature*.

virus protection – защита от вирусов, антивирусная защита # осуществляется с помощью антивирусного ПО (антивируса, *virus-protection software*) или аппаратно-программно с помощью специальной платы, устанавливаемой в ПК. Синоним – *antivirus protection* (см. также *antivirus, virus, virus filtering, virus infection, virus scanner*).

virus-protection software – антивирусное ПО # синоним – *antivirus software*.

virus reporting – оповещение о вирусе # например, real-time virus reporting – оповещение о вирусе, производимое в реальном времени (см. также *virus*).

virus scanner (*также* **anti-virus scanner**) – программа поиска вирусов, антивирусный сканер # вид антивирусного ПО, например, Dr. Web (компании "Доктор Веб"), Norton AntiVirus (Symantec), или AVP ("Лаборатория Касперского"). Выполняет просмотр ОЗУ, загрузочных секторов дисков, файлов и содержимого почтовых ящиков на наличие сигнатур известных вирусов. Недостаток сканеров – неспособность обнаруживать неизвестные (новые) вирусы (см. также *antivirus software, virus, virus reporting, virusscanning schedule*).

virus scanning schedule – регламент антивирусного сканирования # определяет периодичность и время запуска на исполнение программ поиска вирусов на корпоративных компьютерах (см. также *virus scanner*).

virus signature – сигнатура вируса # отличительный признак, обнаруженный у конкретного экземпляра вируса, например участок кода или контрольная сумма; служит для идентификации этого вируса. Для облегчения работы антивирусного ПО, сигнатуры вирусов хранятся в специальных постоянно обновляемых БД (см. также *antivirus software, polymorphic virus, signature, virus*).

virusware (*также* **virware**) – вирусное ПО # программы, распространяющие и/или загружающие (закачивающие) компьютерные вирусы и другие инфекции (см. также *virus*).

viral ransomware – вирусное ПО для вымогательства # вирусная разновидность ПО для вымогательства.

vulnerability (*также* **security vulnerability**) – уязвимость, слабость, слабое место, слабое звено; брешь (дыра) системы защиты (безопасности) # в ИБ и защите данных (ЗД) – свойство системы, позволяющее реализовать соответствующую угрозу; это дефекты безопасности, всё, что может привести к намеренному или случайному нарушению политики безопасности (*security policy*), нарушению работы и/или взлому системы; например, system vulnerabilities – уязвимости системы. В частности, это недостатки и ошибки ПО или аппаратуры (*security error*), которыми может в своих целях воспользоваться злоумышленник. Пример: “I have used both technical and nontechnical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner working” (Kevin D. Mitnik). – Я использовал как технические, так и другие средства, чтобы получить исходные тексты различных ОС и ПО телекоммуникационных систем для изучения их внутреннего устройства и поиска слабых мест. Синонимы – *security breach, security flaw,* security loophole; частичный синоним – *exposure*, антоним – *invulnerability* (см. также *API bug, attack, ethical worm, loophole, security, threat window, vulnerability analysis, vulnerability assessment, vulnerability blocking, vulnerability detection, vulnerability disclosure, vulnerability due to interconnectivity, vulnerability intelligence, vulnerability management, vulnerability scanner, vulnerability surface, window of vulnerability*).

vulnerability analysis – анализ уязвимостей # процесс идентификации и классификации уязвимостей компьютерной системы (см. также *vulnerability, vulnerability assessment*).

vulnerability assessment – оценка уязвимостей # систематическое обследование программной и/или аппаратной системы для определения адекватности действующих средств обеспечения её безопасности, выявления недочётов в защите, сбора данных для прогнозирования эффективности планируемых дополнительных мер безопасности и подтверждения действенности этих мер после их реализации (см. также *security*, *vulnerability, vulnerability analysis*).

vulnerability blocking – блокирование уязвимостей # один из механизмов в системах защиты от вредоносного ПО (см. также *anti-malware, vulnerability*).

vulnerability detection – обнаружение уязвимостей, выявление уязвимостей # синоним – *vulnerability disclosure* (см. также *code analysis, vulnerability*).

vulnerability disclosure – выявление уязвимостей, раскрытие уязвимостей # см. также *disclosure, hacker-powered security*, *vulnerability detection*.

war dialing attack (*также* **war-dialing attack**, **war-dialing**, **war-dial**) – атака через телефонную линию (через модем) # обнаружение неавторизованных модемов (unauthorized modem) путём последовательного прозвона всех номеров телефонов корпорации с целью проникновения в корпоративную сеть; часто сочетается с проверкой на наличие в сети уязвимостей. Синоним – dial-in penetration attack (см. также *CPT, dial-in attack, ethical hacking, penetration testing, security*, *war dialer*).

Web attack – атака через Web, веб-атака # см. также *attack*.

Web security (*также* **web security**) – 1. веб-безопасность; Интернет-безопасность # например, web application security – безопасность веб-приложений. Синонимы – *Internet security, online security* (см. также *security*);
2. защита от Интернет-угроз # защита от веб-угроз (*web threat*), проникающих в корпоративную или домашнюю сеть через Интернет-шлюзы (см. также *attack, exploit, malware, secure web gateway, security, threat, semantic attack, vulnerability, Web security solution*).

whaling (*также* **whale phishing**) – мошенничество с крупными целевыми фигурантами (жертвами, объектами) # разновидность мошенничества или фишинга, направленная на пользователей высокого социального уровня – это обычно крупные бизнесмены, политики, различные знаменитости. Для выуживания персональной и/или коммерческой (финансовой) информации злоумышленники применяют, как правило, методы социальной инженерии (см. также *social engineering, fraud, phishing*);

white-box attack – атака уровня белого ящика # в ИБ – атака, предпосылкой для которой является возможность атакующего-злоумышленника проанализировать программный код приложения, получать доступ к соответствующим адресам памяти во время исполнения программы, вмешиваться в ход программы, перехватывать системные вызовы, использовать для атаки самые разные инструменты (отладчики, эмуляторы и др.). Защиту от атак подобного рода призвана обеспечивать криптография белого ящика (*white-box cryptography*) (см. также *attack, cryptography, system call, white box*).

white hat hacker – этический (белый) хакер # специалист-консультант, помогающий выявлять и устранять уязвимости сетей и систем, обеспечивать ИБ (см. также *ethical hacking*).

zero-day protection – защита от новейших эксплойтов (уязвимостей ПО) # например, zero-day protection scheme – схема защиты от новейших уязвимостей ПО. Для электронной почты – это фиксация резкого увеличения числа входящих писем (incoming emails), обнаружение новых видов спама (см. также *zero-day threat detection*).

zero-day threat detection – обнаружение сегодняшней (сиюдневной, новейшей) угрозы [ПО] # см. также *attack, exploit, threat detection, zero-day protection, zero-day vulnerability*.

zero-day vulnerability (*также* **zero-day**) – сегодняшняя (новейшая) уязвимость [ПО] # только что обнаруженная уязвимость ПО, о которой ещё не известно производителю или для устранения которой ещё нет заплатки. В интересах компьютерного сообщества и пользователей тот, кто обнаружил уязвимость, должен сообщить об этом разработчику и всему сообществу, чтобы можно было как можно быстрее исправить ошибку и/или обеспечить защиту и уменьшение потерь от её вредоносного использования злоумышленниками (см. также *0-day exploit, patch*).

zombie computer (*также* **zombie**, **zombie machine**) – зомбированный компьютер, [компьютер-]зомби # подключённый к Интернету компьютер, атакованный (захваченный) хакером, заражённый вирусом или троянцем. Как правило, это один из компьютеров целой зомбированной сети (*botnet*), которая обычно используется для неблаговидных целей. При этом большинство владельцев таких компьютеров могут даже не знать, что их системы выполняют вредоносные задачи под дистанционным управлением злоумышленников – рассылают спам (согласно оценочным данным, 80% всего спама в мире посылают зомбированные компьютеры), атакуют веб-сайты, участвуют в майнинге криптовалюты и т. д. (см. также *zombie network*).

zombie network – зомби-сеть, сеть зомбированных компьютеров (систем) – см. *botnet*.

6. Список литературы

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 02.07.2021) "Об образовании в Российской Федерации"
2. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму».
4. Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
5. Указ Президента РФ от 30.11.1995 N 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне".
6. Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне".
7. Постановление Правительства Российской Федерации от 06.05.2016 № 399 "Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса".
8. Приказ Министерства труда и социальной защиты Российской Федерации от 31.05.2022 № 331н "Об утверждении типовых дополнительных профессиональных программ повышения квалификации в области противодействия коррупции".
9. Приказ Минтруда РФ от 08.08.2022 N 472Н "Об утверждении профессионального стандарта "Специалист в сфере предупреждения коррупционных правонарушений".
10. Приказ Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств".
11. ГОСТ Р 50922-2006 «Защита информации Основные термины и определения».
12. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности».

7.Итоговый тест

Вопрос 1

Под информационной безопасностью понимается:

Нет верного ответа

Программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая).

Вопрос 2

К правовым методам, обеспечивающим информационную безопасность, относятся:

Разработка аппаратных средств обеспечения правовых данных

Разработка и установка во всех компьютерных правовых сетях журналов учета действий

Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Вопрос 3

Основными источниками угроз информационной безопасности являются все указанное в списке:

Хищение жестких дисков, подключение к сети, инсайдерство

Перехват данных, хищение данных, изменение архитектуры системы

Хищение данных, подкуп системных администраторов, нарушение регламента работы

Вопрос 4

Виды информационной безопасности:

Персональная, корпоративная, государственная

Клиентская, серверная, сетевая

Локальная, глобальная, смешанная

Вопрос 5

Когда получен спам по e-mail с приложенным файлом, следует:

Прочитать приложение, если оно не содержит ничего ценного – удалить

Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

Удалить письмо с приложением, не раскрывая (не читая) его

Вопрос 6

Наиболее распространены угрозы информационной безопасности корпоративной системы:

Покупка нелицензионного ПО

Ошибки эксплуатации и неумышленного изменения режима работы системы

Сознательного внедрения сетевых вирусов

Вопрос 7

Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

Программные, технические, организационные, технологические

Серверные, клиентские, спутниковые, наземные

Личные, корпоративные, социальные, национальные

Вопрос 8

Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования

Моральный износ сети, инсайдерство

Сбой (отказ) оборудования, нелегальное копирование данных

Вопрос 9

Системой криптографической защиты информации является:

BFox Pro

CAudit Pro

Крипто Про

Вопрос 10

Под какие системы распространение вирусов происходит наиболее динамично:

Windows

Mac OS

Android

Вопрос 11

Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?

Регламентированной

Правовой

Защищаемой

Вопрос 12

Утечка информации в системе:

Это ситуация, которая характеризуется потерей данных в системе

Это ситуация, которая характеризуется изменением формы информации

Это ситуация, которая характеризуется изменением содержания информации

Вопрос 13

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:

Снизить уровень классификации этой информации

Улучшить контроль за безопасностью этой информации

Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

Вопрос 14

Определите наиболее распространенные угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования

Моральный износ сети, инсайдерство

Сбой (отказ) оборудования, нелегальное копирование данных

Вопрос 15

Таргетированная атака — это:
Атака на сетевое оборудование
Атака на компьютерную систему крупного предприятия
Атака на конкретный компьютер пользователя

Вопрос 16
Конфиденциальностью называется:
Защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
Описание процедур
Защита от несанкционированного доступа к информации

Вопрос 17
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
Владельцы данных
Руководство
Администраторы

Вопрос 18
Информационная безопасность зависит от:
Компьютеров, поддерживающей инфраструктуры
Пользователей
Информации

Вопрос 19
Какие вирусы активизируются в самом начале работы с операционной системой:
Загрузочные вирусы
Троянцы
Черви

Вопрос 20
Какие угрозы безопасности информации являются преднамеренными:
Ошибки персонала
Открытие электронного письма, содержащего вирус
Не авторизованный доступ