| Термин | Определение |
|---|---|
| **Информационная безопасность** | **Состояние информации при соблюдении конфиденциальности, целостности и доступности.** |
| **Кибербезопасность** | **Подмножество информационной безопасности**<br>**Совокупность мер по защите информационных систем, сетей и цифровых сервисов от вредоносных воздействий с помощью средств ИТ (кибератаки, цифровые каналы и пр.)** |
| **Защита** | **Набор мер (прикладных действий) по обеспечению информационной безопасности** |
| **Конфиденциальность информации** | **Свойство (постулат) информации быть доступной только для авторизованных субъектов (пользователей информации).** |
| **Доступность информации** | **Свойство (постулат) информации быть доступной от авторизованных субъектов в то время, когда она необходима для использования.** |
| **Целостность информации** | **Свойство (постулат) информации быть неискаженной и полной (истинной) без несанкционированных искажений и изменений.** |
| **Идентификация** | **Процесс узнавания субъекта по предоставленному идентификационному признаку (имя учетной записи, устройство, адрес и пр.)** |
| **Аутентификация** | **Процесс проверки соответствия идентификационного признака с представленным подтверждением (имя учетной записи И пароль, устройство И ключ и пр.)** |
| **Авторизация** | **Процесс выдачи атрибутов доступа субъекту после успешной аутентификации (предоставление прав доступа) на возможность выполнения определенных действий (операций).** |
| **Права доступа** | **Набор разрешенных и запрещенных операций в некоторой системе (например, права чтения на файл или каталог, возможность выполнения определенного действия в системе и пр.)** |
| **Роль пользователя** | **Совокупность прав доступа субъекта, ассоциируемая с некоторым названием ("Администратор рабочей станции", "Пользователь", "Разработчик" и пр.)** |
| **Учетная запись** | **Совокупность идентификатора субъекта и атрибутов в некоторой системе (имя учетной записи, роль или права доступа, параметры и ограничения)** |
| **Пароль** | **Фраза, которую "знает" пользователь (владелец идентификатора), состоящая из букв, цифр и других печатаемых символов, необходимая для процесса аутентификации (если производится аутентификация по паролю).** |
| **Фактор аутентификации** | **Средство аутентификации пользователя (пароль, одноразовый код, устройство, ключ и др.), подразделяемые на "что знаю" (пароль), "чем владею" (устройство), "кем являюсь" (биометрия)** |
| **Двухфакторная аутентификация** | **Процесс аутентификации с использованием двух различных факторов аутентификации (пароль И устройство, пароль И биометрия)** |
| **Многофакторная аутентификация** | **Процесс аутентификации с использованием более двух различных факторов аутентификации (пароль И устройство И биометрия)** |

| | |
|---|---|
| **Дву- или много-ступенчатая аутентификация** | **Процесс аутентификации с двумя или более одинаковыми факторами аутентификации (два разных пароля), выполняемых последовательно (по шагам).** |
| **Сторонняя аутентификация** | **Процесс аутентификации с использованием внешней (сторонней) системы аутентификации (OAuth, Windows-аутентфикация, Аутентификация через аккаунт HSE)** |
| **PUSH-код** | **Способ доставки кода аутентификации с помощью push-уведомления к доверенному устройству пользователя с установленным приложением.** |
| **SMS-код** | **Способ доставки кода аутентификации с помощью SMS на мобильный номер телефона пользователя (субъекта)** |
| **Одноразовый код** | **Способ использования кода аутентификации, действительный ограниченное время или в рамках одной попытки аутентификации** |
| **Биометрическая аутентификация** | **Фактор аутентификации по уникальным биометрическим характеристикам субъекта (лицо, отпечаток пальцев и пр.)** |
| **Шифрование** | **Преобразование открытого текста с помощью алгоритма шифрования в шифр-текст для обеспечения конфиденциальности хранимой и/или передаваемой информации (текста).**<br>**Для выполнения процесса шифрования обязателен ключ шифрования (может быть симметричным и асимметричным)** |
| **Расшифрование** | **Обратное преобразование шифр-текста с помощью алгоритма шифрования в открытый текст (исходный).**<br>**Для выполнения процесса расшифрования обязателен ключ шифрования (может быть симметричным и асимметричным)** |
| **Алгоритм шифрования** | **Метод (математического) преобразования входной последовательности бит (текста) в другую последовательность бит (шифр-текст).**<br>**AES, DES, ГОСТ и др.**<br>**Иначе называется криптографический алгоритм.** |
| **Шифр-текст** | **Итоговая последовательность бит, получаемая в результате работы алгоритма шифрования, и представленная в виде набора символов (текста).** |
| **Кодирование** | **Преобразование открытого текста в избыточном виде для представления каждого символа из текста однозначным представлением в виде ограниченного набора символов (исключаются управляющие и непечатаемые символы, используются только цифры, буквы английского алфавита и некоторые знаки пунктуации).**<br>**Алгоритм Base64. Для выполнения кодирования не требуется ключ шифрования, то есть это преобразование не обеспечивает конфиденциальность при хранении и передаче.** |
| **Декодирование** | **Обратное преобразование закодированного текста в открытый текст. Для выполнения декодирования не требуется ключ шифрования, то есть это преобразование может выполнить любой субъект (пользователь).** |
| **Хэширование** | **Одностороннее преобразование информации (открытого текста) в некоторое значение (хэш) фиксированной длины.**<br>**Восстановление данных обратным преобразованием невозможно. Чтобы выяснить содержимое исходного открытого текста нужно произвести перебор всех вариантов, что трудоемко и занимает огромное время.** |

| | |
|---|---|
| | **Хэширование используется для подтверждения неизменности (целостности) открытого текста, хранения хэшей паролей и пр.** |
| **Хэш** | **Результат хэширования, то есть некоторое значение фиксированной длины.** |
| **Угроза** | **Потенциальная возможность определенным образом нарушить информационную безопасность.** |
| **Кража, утечка** | **Разглашение информации, нарушение конфиденциальности.<br>Кража - умышленное хищение информации.<br>Утечка - несанкционированный/случайный выход информации за пределы информационной системы.** |
| **Взлом** | **Применение активных действий по нарушению средств защиты информации для осуществления несанкционированного доступа к информации.** |
| **Атака** | **Автоматизированные действия (Целенаправленное действие), направленные на использование уязвимостей в системе, для осуществления несанкционированного доступа к информации** |
| **Авария** | **Выход из строя аппаратного или программного обеспечения нештатным образом** |
| **Угроза конфиденциальности** | **Потенциальная возможность воздействия нарушения конфиденциальности, т.е. несанкционированного доступа по любым причинам** |
| **Угроза доступности** | **Потенциальная возможность воздействия нарушения доступности, т.е. привести систему в состояние "отказ в обслуживании" (отказ в доступе) по любым причинам** |
| **Угроза целостности** | **Потенциальная возможность воздействия нарушения целостности хранимой и обрабатываемой информации, т.е. искажение, уничтожение, повреждение и пр.** |
| **Источник угроз** | **Исходные причины потенциального воздействия на безопасность информации** |
| **Антропогенный источник угроз** | **Источник угроз, связанный с человеком, то есть источник угроз - действия (или бездействие) человека.** |
| **Техногенный источник угроз** | **Источник угроз, связанный с техническим обеспечением (аппаратным или программным).** |
| **Стихийный источник угроз** | **Источник угроз, связанный со стихийными природными явлениями (ураган, снегопад, ливень, паводок, шторм и пр.)** |
| **Внешние угрозы** | **Угрозы, на которые владелец системы не может повлиять непосредственно (законодательная база, различные конфликты и пр.)** |
| **Внутренние угрозы** | **Угрозы, на которые владелец системы может влиять (архитектура, используемое оборудование и ПО и пр.)** |
| **Уязвимость** | **Причина, приводящая (или которая может привести) к нарушению безопасности информации** |
| **Последствие** | **Результат реализации угрозы Ущерб, штраф, нарушение ИБ** |
| **Нарушитель** | **Лицо, которое может использовать использовало или использует уязвимости и реализовать угрозы** |

| | |
|---|---|
| **Внутренний нарушитель** | **Нарушитель, являющийся сотрудником (или работником) организации, т.е. находится "внутри" инфраструктуры организации (на ее территории)** |
| **Внешний нарушитель** | **Нарушитель, НЕ являющийся сотрудником (или работником) организации, и находящийся вне инфраструктуры организации.** |
| **Мотив нарушителя** | **Причина действий нарушителя.<br>Безответственность, самоутверждение, корыстный интерес** |
| **Модель угроз** | **Систематизированный перечень актуальных угроз безопасности информации при их обработке в информационной системе** |
| **Банк данных угроз** | **БДУ ФСТЭК. Централизованная база данных об актуальных угрозах безопасности и уязвимостях программного обеспечения.** |
| **Каталог уязвимостей** | **CVE, БДУ ФСТЭК, Vulners и др. Структурированный перечень/реестр выявленных недостатков в программном или аппаратном обеспечении, которые могут быть использованы злоумышленниками для нарушения безопасности системы** |