Такие технологии, как IoE и GIS, способствуют накоплению огромных объемов данных. Назовите две причины, в силу которых эти технологии увеличивают спрос на специалистов по кибербезопасности. (Выберите два варианта.)

**С помощью этих технологий ведется сбор конфиденциальной информации.**

**В системах, созданных на основе этих технологий, хранятся персональные данные.**

В каких трех состояниях данные уязвимы для атак? (Выберите три варианта.)

**обрабатываемые данные**

**передаваемые данные**

**хранимые данные**

Назовите технологию, с помощью которой можно было бы в принудительном порядке обеспечить соблюдение политики безопасности, согласно которой вычислительное устройство может быть подключено к сети комплекса зданий лишь при условии, что на этом устройстве установлено последнее обновление антивирусного ПО.

**NAC**

Какую технологию идентификации можно использовать в составе системы аутентификации сотрудников?

**считывание смарт-карт**

Назовите нетехнический метод, с помощью которого киберпреступники получают конфиденциальную информацию.

**социальная инженерия**

Какое из описаний точнее всего соответствует DDoS-атаке?

**Злоумышленник формирует ботнет из компьютеров-зомби.**

Руководящий сотрудник компании отправился на важную встречу. Через некоторое время его секретарю звонят и сообщают, что руководитель будет вести важную презентацию, но файлы этой презентации повреждены. Звонящий настойчиво просит секретаря немедленно переслать презентацию на личный адрес электронной почты. Неизвестный также утверждает, что руководитель возлагает ответственность за успех презентации непосредственно на секретаря. К какому типу относится такая тактика социальной инженерии?

**Принуждение**

Подразделению ИТ поручили внедрить систему, которая будет контролировать полномочия пользователей в корпоративной сети. Какое решение следует применить в этом случае?

**набор атрибутов, описывающих права доступа пользователя**

Пользователь хранит большой объем конфиденциальных данных, которые необходимо защитить. Какой алгоритм лучше подходит для решения этой задачи?

**3DES**

Как называется механизм безопасности, к которому относятся пароли, парольные фразы и PIN-коды?

**Аутентификация**

К какому типу средств контроля доступа относятся смарт-карты и системы биометрической идентификации?

**Логические**

Какие средства контроля доступа должны будут применить сотрудники подразделения ИТ, чтобы восстановить нормальное состояние системы?

**Корректирующие**

Какой алгоритм применяется в Windows по умолчанию при шифровании файлов и папок на томе NTFS?

**АES**

Назовите технологию, с помощью которой можно предотвратить атаку, реализуемую методом перебора по словарю или методом грубой силы с использованием хеш-суммы?

**HMAC**

В организации будет развернута сеть VPN, через которую пользователи смогут безопасно получать удаленный доступ к корпоративной сети. Назовите компонент, с помощью которого в IPsec производится аутентификация источника каждого пакета для проверки целостности данных.

**HMAC**

Какую технологию следует внедрить, чтобы иметь возможность идентифицировать организацию, выполнить аутентификацию веб-сайта этой организации и установить зашифрованное соединение между клиентом и веб-сайтом?

**цифровой сертификат**

Технические специалисты проверяют безопасность системы аутентификации, где применяются пароли. Проверяя таблицы паролей, один из специалистов видит, что пароли сохранены в виде хеш-сумм. Сравнив хеш-сумму простого пароля с хеш-суммой того же пароля из другой системы, специалист обнаруживает, что хеш-суммы не совпадают. Назовите две вероятные причины такого несовпадения. (Выберите два варианта.)

**В системах применяются различные алгоритмы хеширования.**

**В одной системе применяется только хеширование, тогда как в другой системе, помимо хеширования, применяется механизм добавления соли.**

Назовите системы раннего оповещения, которые можно использовать в борьбе с киберпреступниками.

**Проект Honeynet**

Как называется атака, при которой данные превышают объем памяти, отведенной приложению?

**переполнение буфера**

Как называется атака, при которой злоумышленник выдает себя за авторизованную сторону и пользуется уже существующими доверительными отношениями между двумя системами?

**Подмена**

Вам поручили провести работу с сотрудниками, отвечающими за сбор и ввод данных в вашей организации: нужно улучшить контроль целостности данных при вводе и модификации. Некоторые сотрудники просят объяснить, с какой целью в новых формах для ввода данных введены ограничения по типу и длине вводимых значений. Что из перечисленного можно назвать новым средством контроля целостности данных?

**правило проверки ввода, гарантирующее полноту, точность и непротиворечивость данных**

В организации только что завершили аудит безопасности. Согласно результатам аудита, в вашем подразделении не обеспечено соответствие требованиям стандарта X.509. Какие средства контроля безопасности нужно проверить в первую очередь?

**цифровые сертификаты**

Алиса и Боб подписывают документы, пользуясь технологией цифровой подписи. Каким ключом Алиса должна подписать документ, чтобы Боб смог удостовериться в том, что этот документ действительно поступил от Алисы?

**закрытый ключ Алисы**

Назовите главную особенность криптографической хеш-функции.

**хеш-функция необратима.**

В организации устанавливают только те приложения, которые соответствуют внутренним нормам. Все остальные приложения удаляются администраторами в целях усиления безопасности. Как называется этот метод?

**стандартизация ресурсов**

Понимание и выявление уязвимостей относятся к числу важнейших задач специалиста по кибербезопасности. Назовите ресурсы, с помощью которых можно получить подробную информацию об уязвимостях.

**Национальная база данных общих уязвимостей и рисков (CVE)**

Назовите подход к обеспечению доступности, при котором используются разрешения на доступ к файлам?

**Ограничение**

Группа специалистов проводит анализ рисков применительно к сервисам БД. Помимо прочего, специалисты собирают следующую информацию: первоначальная ценность ресурсов; существующие угрозы для этих ресурсов; ущерб, который могут нанести эти угрозы. На основании собранной информации специалисты рассчитывают ожидаемый годовой объем убытков. Какой вид анализа рисков выполняет группа?

**количественный анализ**

Риск-менеджер вашей организации представил схему, где уровни угрозы для ключевых ресурсов систем информационной безопасности обозначены тремя цветами. Красный, желтый и зеленый цвета обозначают соответственно высокий, средний и низкий уровень угрозы. Какому виду анализа рисков соответствует такая схема?

**качественный анализ**

Какой инструмент Windows следует использовать для настройки политики паролей и политики блокировки учетных записей в системе, которая не входит в домен?

**Оснастка «Локальная политика безопасности»**

Какой протокол следует применить, чтобы обеспечить безопасный удаленный доступ для сотрудников, находящихся дома?

**SSH**