3 вариант

Деменчук Георгий ПИ19-3

Задача 1

**Какие две статьи, и какой части Гражданского кодекса РФ относятся к защите данных? Какая ответственность может возникать при нарушении этих статей, и в чем она будет заключаться?**

Глава 8 — Нематериальные блага и их защита

Статья 152 — Удаление информации, денежная компенсация

Статья 150 — Возврат благ, денежная компенсация

Задача 2

**Вы оператор персональных данных в РФ... Какие меры вы должны предпринять согласно ПП1119? Какого класса устройства СЗИ от НСД вы должны приобрести? Средства какого уровня криптографической защиты вы должны использовать?**

1) Обеспечить безопасность персональных данных

2) Выбрать средство защиты информации в соответствии с нормативными правовыми актами

3) Определение типа угроз безопасности персональных данных, актуальных для информационной системы

4) Контроль за выполнением настоящих требований

Какого класса устройство СЗИ от НДС вы должны приобрести?

В информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

Средства какого уровня криптографической защиты вы должны использовать?

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе

**Задача 3**

**Перечислите актуальные угрозы IOT. Объясните, почему они актуальны.**

1. стандартные учётные записи от производителя, слабая аутентификация

2. отсутствие поддержки со стороны производителе для устранения уязвимостей

3. трудно или невозможно обновить ПО и ОС

4. использование текстовых протоколов и ненужных открытых портов

5. используя слабость одного гаджета, хакеру легко попасть во всю сеть

6. использование незащищённых мобильных технологий

7. использование незащищённой облачной инфраструктуры

8. использование небезопасного ПО

В ходе проведенного HP исследования обнаружено, что примерно в 70% проанализированных устройств не шифруется беспроводной трафик. Веб-интрефейс 60% устройств эксперты HP посчитали небезопасным из-за небезопасной организации доступа и высоких рисков межсайтового скриптинга. В большинстве устройств предусмотрены пароли недостаточной стойкости. Примерно 90% устройств собирают ту или иную персональную информацию о владельце без его ведома.

**ТЕСТ**

Задача 1

Какие две статьи, и какой части ГК РФ относятся к защите данных? Какая ответственность

Какие исключения предусматривает закон РФ о защите персональных данных в области хранения и распространения ПД?

**- Международные требования**

**- ПД хранящиеся в Архивном фонде РФ**

**- Требования закона 262-ФЗ**

- Требования закона 114-ФЗ

**- Требования закона 57-ФЗ**

В какие страны не могут передавать персональные данные российские операторы ПД?  
1. Аргентина

**2. США**

3. Марокко

4. Грузия

5. Норвегия

6. **Калифорния** – это не страна, но входит в США

Почему?

Данных стран нет в списке стран на основании закона от 05.08.2022 № 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных"

Какие Российские службы из списка ответственны за ИБ РФ?

- Министерство обороны

**- Министерство связи**

- Министерство труда и социальной защиты

**- Минюст**

- Роспечать

Какие еще государственные организации РФ являются ответственными за соблюдение ИБ?

**ФСБ России**

**ФСТЭК**

**ГосСОПКА**

**Роскомнадзор**

Какой уязвимости ИС нет в списке?

Уязвимость кода

Уязвимость конфигурации

Уязвимость архитектуры

Уязвимость СЗИ

Уязвимость архитектуры

**Организационная уязвимость** - Уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации информационной системы, требований организационно-распорядительных документов по защите информации и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственным за защиту информации.

Чем идентификация отличается от аутентификации? Какие из принятых видов двухфакторной аутентификации не являются настоящей двухфакторной? Почему?

**Идентификация** — это процедура распознавания пользователя по его личному идентификатору. Эта функция выполняется при попытке пользователя войти в сеть. **Аутентификация** — это процедура проверки подлинности заявленного пользователя, процесса или устройства

- ОТР Токен и пароль – также используется, например для доступа к 1С

- **Механизм challenge-response и приложение на телефоне**

- Пароль и SMS одноразовый пароль – точно является и используется

Что такое single sign on? Перечислите аргументы за и против. Что такое ААА сервер? Приведите пример.

**Технология единого входа (Single sign-on SSO)** — метод аутентификации, который позволяет пользователям безопасно аутентифицироваться сразу в нескольких приложениях и сайтах, используя один набор учетных данных.

**AAA-сервер** обеспечивает аутентификацию, авторизацию и учёт, управление сессиями абонентов в режиме реального времени для обеспечения мобильности, роуминга, безопасности и контроля за используемыми услугами и сервисами.

Опишите хотя бы две любые из моделей ролевого доступа

Модель ролевого управления доступом (RBAC – Role-based Access Control), также называемая недискреционным управлением доступом (Nondiscretionary Access Control), использует централизованно администрируемый набор контролей, предназначенных для определения порядка взаимодействия субъекта с объектом. Этот тип модели разрешает доступ к ресурсам, основываясь на роли пользователя в компании. Это называют недискреционным подходом, поскольку назначение пользователю роли является неизбежным. Вы не определяете самостоятельно, какая роль вам будет назначена.

Существует два типа иерархий:

* Ограниченные иерархии – доступен только один уровень иерархии.
* Обычные иерархии – доступно много уровней иерархии.

Хеширование

**Зачем нужен криптографический хеш?**

Хеширование чаще всего используется для проверки целостности данных файлов и аутентификации пользователя.

**Какие у него свойства?**

Основное свойство – детерминированность: одно и то же входное значение всегда будет выдавать одно и то же выходное значение.

Коллизия – разные входные наборы байт могут выдавать одинаковые хеши. Чем меньше коллизий в хеш-функции, тем лучше.

Скорость вычисления – чем быстрее вычисляется функция, тем лучше. Для наиболее популярных хеш-алгоритмов существует аппаратная поддержка на уровне инструкций процессоров на архитектурах 86 и ARM.

**Где он используется?**

- В антивирусах для поиска сигнатур вредоносных файлов

- Для защиты файлов (.7z, .rar)

- Аутентификация на сайтах

-Проверка целостности данных файлов

**Можно ли использовать криптографический хеш для обезличивания ПД?**

Особенность хеша заключается в том, что в стандартном его применении хеширование возможно только в одну сторону.

Обычно, когда мы используем какие-либо персональные данные, то мы предполагаем, что они нам нужны для последующей обработки и анализа. В случае применения хеш-функции обратное преобразование затруднительно, поэтому обычно хеширование персональных данных не используется.

Что такое радужные таблицы и зачем они используются.

Т.к. обычно в хеш-функциях достаточно малая коллизия, то можно подать на вход много слов и аккумулировать полученные результаты, тем самым составить ассоциативные массивы вида:

{“слово”: “хеш”}

Это и называется хеш-таблицей, тем самым возможно подобрать пароль для хеша.

Для генерации радужной таблицы необходимо большое пространство на SSD и высокая степень чтения/записи на носитель

Для вычисления уже по созданной радужной таблице особо больших мощностей видеоускорителя/cpu не требуется.

Зачем нужна соль?

Соль как раз нужна для того, чтоб избежать взлома хеша по радужной таблице. Соль видоизменяет хеш и становится труднее подобрать обратные ему данные.

Перечислите стойкие на сегодняшний день хэш алгоритмы.

SHA-256

SHA-3 (Keccak)

ГОСТ Р 34.11-2012 (Стрибог).

Почему в алгоритмах одноразовых паролей MOTP, TOTP, HOTP можно использовать не стойкий хэш алгоритм?

Т.к. обычно одноразовые пароли живут достаточно малое кол-во времени (несколько минут, часов), то взламывать подобные данные потенциальному злоумышленнику нецелесообразно.

4. Опишите кратко AES: что это за стандарт, зачем он, является ли он стойким

AES – блочный шифр с длиной блоков равной 128 битам, и шифр поддерживает ключи длиной N, равной 128, 192 или 256 бит.

Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES.

Шифрование AES-256 более стойкое, чем RSA 512. AES-128 не является стойким, AES-256 является стойким.

5. Опишите кратко актуальный российский стандарт электронной подписи

ГОСТ 34.10-2018 — действующий межгосударственный криптографический стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи, реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.

Криптографическая стойкость первых стандартов цифровой подписи ГОСТ Р 34.10-94 и ГОСТ 34.310-95 была основана на задаче дискретного логарифмирования в мультипликативной группе простого конечного поля большого порядка.

Начиная с ГОСТ Р 34.10-2001 стойкость алгоритма основана на более сложной задаче вычисления дискретного логарифма в группе точек эллиптической кривой. Также стойкость алгоритма формирования цифровой подписи основана на стойкости соответствующей хеш-функции.