Максимальный балл за работу – 20.

1. Из определения информационной безопасности известно, что безопасность информации обеспечивается, когда соблюдаются свойства безопасности – конфиденциальность, целостность и доступность. Конфиденциальность – свойство, отвечающее за то, что доступ к информации имеется только при наличии разрешения или факта владения этой информацией.

Какая ситуация относится к нарушению конфиденциальности?

1. Атакующий смог украсть финансовые сведения из базы данных малого регионального банка.
2. Атакующий смог удалённо поменять настройки базы данных так, чтобы сотрудники не могли зайти в информационную систему.
3. Атакующий смог удалённо уничтожить данные (например, вирусом-вайпером) в базе данных организации.
4. Атакующий смог убедить системного администратора компании создать аккаунт для атакующего с повышенными привилегиями в системе.

2. Из определения информационной безопасности известно, что безопасность информации обеспечивается, когда соблюдаются свойства безопасности – конфиденциальность, целостность и доступность. Целостность – свойство, отвечающее за состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно лицами, имеющими на него право.

Какая ситуация относится к нарушению целостности?

1. Атакующий смог украсть сведения из базы данных малого регионального банка.
2. Атакующий смог удалённо поменять настройки базы данных так, чтобы сотрудники не могли зайти в информационную систему.
3. Атакующий смог удалённо уничтожить данные (например, вирусом-вайпером) в базе данных организации.
4. Атакующий смог убедить системного администратора компании создать аккаунт для атакующего с повышенными привилегиями в системе.

3. Из определения информационной безопасности известно, что безопасность информации обеспечивается, когда соблюдаются свойства безопасности – конфиденциальность, целостность и доступность. Доступность информации - свойство, отвечающее за состояние информации, при котором лица, имеющие права доступа к информации, могут реализовать их беспрепятственно.

Какая ситуация относится к нарушению доступности?

1. Атакующий смог украсть сведения из базы данных малого регионального банка.
2. Атакующий смог удалённо поменять настройки базы данных так, чтобы сотрудники не могли зайти в информационную систему.
3. Атакующий смог удалённо уничтожить данные (например, вирусом-вайпером) в базе данных организации.
4. Атакующий смог убедить системного администратора компании создать аккаунт для атакующего с повышенными привилегиями в системе.

4. После установки скаченной из Интернета программы с компьютера пропали все фотографии. Наиболее вероятная причина**:**

1. Случайное удаление
2. Сбой памяти
3. Внезапное обновление системы
4. Вредоносная программа

5. Ты в открытом чате опубликовал расписание уроков своей школы с указанием класса и ФИО учителя. Это может привести к утечке:

1. Служебной информации
2. Персональных данных
3. Технических данных
4. Открытых данных

6. Одним из видов вопросов, которыми занимается такая наука как информационная безопасность, является вопрос выдачи и управления доступами к информации. Процесс выдачи доступа делится на три этапа – идентификацию, аутентификацию и авторизацию. Идентификация – проверка идентификатора субъекта, что он принадлежит информационной системе организации. Идентификатор – уникальное значение, которое назначается субъекту, используется только им, и оно не должно указывать на свойства или суть занимаемой должности.

Какой из вариантов описывает ситуацию, когда идентификатор используется неправильно?

1. Системный администратор Алексей имеет два логина (идентификатора) в системе свой организации – логин alex_e1a2ffde он использует для управления серверами, а alex_fe9081cb использует для отправки и чтения писем.
2. Специалист по подбору персонала Алёна использует идентификатор alyona_1995@gmail.com для общения в специальной соцсети HR-ов.
3. Бухгалтеры Лада и Елизавета используют один и тот же логин руководителя бухгалтерии dmitry_finances\personal.org в целях упрощения свой деятельности и для использования электронно-цифровой подписи руководителя.
4. Специалист мониторинга службы информационной безопасности Артём использует один и тот же логин a.deberov для чтения почты и использования общих ресурсов для обучения персонала компании.

7. Какой из способов аутентификации относится к многофакторной?

1. Использование только пароля
2. Использование пароля и отпечатка пальца
3. Использование только PIN-кода
4. Использование только QR-кода

8. Какой вектор атаки чаще всего используется при целевых фишинговых кампаниях?

1. Массовая рассылка по известным адресам почты
2. Социальная инженерия через персонализированные письма
3. Использование эксплойтов для удалённого кода без взаимодействия с пользователем
4. DDoS на инфраструктуру цели

9. Какой из перечисленных видов атакующего обычно описывает хорошо финансируемую, долгосрочную и целенаправленную операцию с высокой степенью скрытности и доступом к значительным ресурсам?

1. Скрипт-кидди
2. Внутренний злоумышленник
3. APT (Advanced Persistent Threat)
4. Группа хактивистов

10. Соотнесите названия и цель информационных ресурсов. В ответ выпишите пары вида 1-Б, 2-А и т.д., без запятых. Пример ответа: "1-А 2-Б 3-В"

1. MITRE ATT&CK (https://attack.mitre.org/)	А) Реестр публично идентифицированных уязвимостей с уникальными идентификаторами и ссылками на эксплойты/исправления
2. CVE: Common Vulnerabilities and Exposures https://www.cve.org/	Б) Ресурс, содержащий методики, руководства и проекты по веб-безопасности (топы уязвимостей, тесты, практические инструменты).
3. OWASP Foundation https://owasp.org/	В) База знаний по тактикам, техникам и процедурам атак для моделирования и обнаружения угроз.

11. Петя проверил настройки сети на своем компьютере и увидел:

IP-адрес: 192.168.10.77

Маска подсети: 255.255.255.240

Сколько всего устройств может быть в одной сети с его компьютером?

12. Петя выбирает для своего сайта правила по созданию пароля доступа для зарегистрированных пользователей. Первый вариант – 8 строчных английских букв, второй вариант – 6 символов из набора (английский буквы (большие и маленькие) и цифры). Какой пароль будет надежнее от взлома полным перебором? В ответ напишите “1” или “2”.

Дан набор символов, которым сокрыто осмысленное слово на русском языке:

$! ! ! _ _ # _ & ! ! _

Известны комбинации символов, соответствующие некоторым буквам русского алфавита:

! ! _	_ #	! _	$! !	_ # _	& !	&	!	_	$!	#
А	Б	Е	З	Й	К	Н	Р	С	Т	Ч

13. Какое слово было зашифровано?
14. Сколько букв в зашифрованном слове из предыдущего задания?
15. Зашифруй слово **БЕРЕСТА**, используя таблицу замены букв на специальные символы из задания выше.

Бланк ответов

ФИО		Класс:	

Задание	Количество баллов за задание	Оценка проверяющего	Ваш ответ
№1	1		
№2	1		
№3	1		
№4	1		
№5	1		
№6	1		
№7	1		
№8	1		
№9	1		
№10	1		
№11	2		
№12	2		
№13	2		
№14	2		
№15	2		
Сумма баллов:			