1. Расшифровать с помощью алгоритма Цезаря закрытый текст.
Закрытый текст – uxghv, ключ – 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

A) rudes
B) fakes
C) torto
D) dorama
E) letty
F) betty

2. Расшифровать с помощью алгоритма Цезаря закрытый текст.
Закрытый текст –swgta, ключ – 2

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

A) query
B) fairy
C) picnic
D) frame
E) carpet
F) learn

3. Расшифровать с помощью алгоритма Цезаря закрытый текст.
Закрытый текст – wrslf, ключ – 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

A) rudes
B) focus
C) topic
D) dream
E) loter
F) barty

4. Расшифровать с помощью алгоритма Цезаря закрытый текст.
Закрытый текст –eduwb, ключ – 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

A) pocus
B) focus
C) team
D) dream
E) mitter
F) barty

5. Аутентификация (Authentication)
A) процедура проверки подлинности входящего в систему пользователя, процесса или устройства по идентификатору
B) процедура предоставления субъекту определенных полномочий и ресурсов в данной системе
C) регистрация действий пользователя в сети, включая его попытки доступа к ресурсам
D) нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация)
E) свойство ресурса или компонента быть неизменным в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий
F) нарушение (частичное или полное) работоспособности системы

6. Односторонняя аутентификация
A) обмен информацией только в одном направлении
B) содержит дополнительный ответ проверяющей стороны доказывающей стороне
C) содержит дополнительную передачу данных от доказывающей стороны проверяющей
D) проверяет расположение данных в четырех направлениях
E) антивирусная программа для проверки уязвимостей и дополнительными средствами мониторинга

7. Технические (программно-технические) меры защиты
   A) меры общего характера, затрудняющие доступ к ценной информации злоумышленникам вне зависимости от особенностей способа обработки информации и каналов утечки и воздействия
   B) меры, связанные со спецификой каналов утечки (воздействия) и метода обработки информации, но не требующие для своей реализации нестандартных приемов, оборудования или программных средств.
   C) меры, жестко связанные с особенностями каналов утечки и воздействия и требующие для своей реализации специальных приемов, оборудования или программных средств.
   D) анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов
   E) комплекс организационных, организационно-технических и технических мер, предотвращающих или снижающих возможность образования каналов утечки информации и/или каналов воздействия на систему.
   F) способы хищения основываются на модификации информации, отображающей электронную наличность
8. Несоответствие программного обеспечения и аппаратных средств принятой политике
   A) не представленна в виде набора документов политика безопасности
   B) частая замена персонала, отвечающего за реализацию политики защиты
   C) недостаточно строго контролируемые процедуры выбора пароля пользователями
   D) неадекватный мониторинг, аудит и несвоевременное устранение проблем сети
   E) несанкционированные изменения топологии сети или установка непроверенных приложений
   F) отсутствие четкого плана обработки инцидентов защиты и восстановления работоспособности сети предприятия в случае сетевой атаки
9. Недостатки конфигурации сетей
   A) недостаточная защита, обеспечиваемая установками по умолчанию
   B) неправильная конфигурация сетевого оборудования
   C) незащищенные учетные записи пользователей
   D) ненадежный пароль
   E) отсутствие аутентификации
   F) ненадежный брандмауэр

10. Атака с использованием множества узлов для осуществления атаки на сервер-жертву
    A) DDoS-атака
    B) DCOM RPC
    C) SMBdie
    D) Мейл-бомбинг
    E) Xspider
    F) MaxPatrol