**Основные правила безопасного поведения в интернет (ознакомься)**

**Надёжные пароли**

Пароли должны быть сложными — минимум 12 символов, включая цифры, заглавные буквы и специальные символы.

**Двухфакторная аутентификация**

Двухфакторная или многофакторная аутентификация работает так: после ввода пароля приложение запрашивает дополнительный код, который приходит в СМС, или сканирует биометрию — отпечаток пальца или лицо. В таком случае украсть данные практически невозможно.

**Пользоваться только своими гаджетами**

Можно попросить у знакомого телефон, чтобы проверить одно сообщение на почте, а потом забыть выйти из аккаунта. Если пришлось воспользоваться чужим гаджетом, не забудьте выйти из своих учётных записей.

**Открывать проверенные ссылки**

Если это не ссылка от хорошо знакомых вам людей лучше её не открывать.

**Беречь личные данные**

Не отправлять личные снимки, адрес прописки и фотографию паспорта людям, которых вы не знаете.

**Регистрироваться на проверенных и только нужных сайтах**

Иначе можно создать много учётных записей, забыть о них — а мошенники могут получить к ним доступ.

**Устанавливать официальные приложения и регулярно их обновлять**

Не скачивать приложения с сомнительных сайтов. Самый безопасный способ — загружать их из магазинов приложений или с официальных сайтов.

**Проверять, какие данные собирает приложение**

После того как приложение установилось, оно может запросить доступ к навигатору, фотографиям, камере. Нужно внимательно проверить, для чего ему эти доступы. Проверяйте, чтобы у приложений не было доступа к микрофону, телефонной книге, СМС.

**Избегать публичных сетей Wi-Fi**

Включайте Wi-Fi и Bluetooth на смартфоне, только когда они нужны — и не забывайте выключать после использования.

**Платить в интернете внимательно**

Они похожи на официальные страницы магазина или сервиса, но в их URL-ссылке всегда есть небольшое несоответствие — например, изменена одна буква. На них можно перейти по ссылкам от незнакомых отправителей или из почтовой рассылки.

На последнем шаге покупки всегда проверяйте, кто получатель. Если это карта физического лица, а не юридическая организация — скорее всего, вас пытаются обмануть.

**Выполни тест**

**Задание 1**

**Основные объекты информационной безопасности:**

а) информационные системы, психологическое состояние пользователей

б) компьютерные сети, базы данных

в) бизнес-ориентированные, коммерческие системы

**Задание 2**

**Ответственность за защищенность данных в компьютерной сети несет:**

а) пользователь сети

б) администратор сети

в) владелец сети

**Задание 3**

**Пароль пользователя должен**

а) содержать только цифры

б) содержать цифры и буквы, знаки препинания и быть сложным для угадывания

в) иметь явную привязку к владельцу, чтобы не забыть пароль (его имя, дата рождения, номер телефона и т.п.)

**Задание 4**

**Электронно-цифровая подпись – это**

а) реквизит электронного документа, предназначенный для защиты данного документа от подделки, позволяющий идентифицировать владельца, а также установить отсутствие искажения информации в электронном документе

б) отсканированная подпись руководителя организации и помещенная в электронный документ для заверения подлинности данного документа

в) такой подписи не бывает т.к. подлинность документа заверяется личной подписью руководителя организации и печатью

**Задание 5**

**Какую ответственность влечет нарушение Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ?**

а) гражданскую ответственность

б) уголовную и административную ответственность

в) дисциплинарную, гражданско-правовую, административную или уголовную ответственность

**Задание 6**

**Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации – это**

а)авторизация

б) идентификация

в) деперсонализация

г) аутентификация

**Задание 7**

**Процесс сообщения субъектом своего имени или номера с целью получения определенных полномочий (прав доступа) на выполнение некоторых действий в системах с ограниченным доступом – это**

а) авторизация

б) идентификация

в) деперсонализация

г) аутентификация

**Задание 8**

**Идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему, называется:** а) логин б) пароль в) доменное имя г) сетевой адрес

**Задание 9**

**Электронная почта позволяет передавать**  
а) только сообщения б) сообщения и вложенные файлы в) видеоизображения  
**Задание 10**

**Устройствами ввода информации являются (выберите несколько вариантов ответа):**  
а) сканер  
б) принтер  
а) монитор  
г) клавиатура  
**Задание 11**

**Поиск информации в Интернете по ключевым словам предполагает:**  
а) ввод слова (словосочетания) в поисковую строку  
б) ввод слова (словосочетания) в адресную строку  
в) переход по гиперссылке с первой загруженной страницы

**Задание 12**

**Что такое токен?**

а) что-то связанное с током

б) код для авторизации

в) вирус

**Задание 13**

**Как лучше хранить пароли?**

а) внести в текстовый файл

б) добавить в менеджер паролей

в) записать на бумажке

**Задание 14**

**Зачем нужны межсетевые экраны?**

а) для контроля доступа между сетями

б) для защиты от спама

в) для защиты от сглаза

**Задание 15**

**Вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ:**

а) кибербуллинг б) электронные риски в) коммуникационные риски

**Задание 16**

**К какому типу Интернет-зависимости относятся бесконечные путешествия по всемирной паутине, поиск информации:**

а) навязчивый веб-серфинг б) пристрастие к виртуальному общению в) игровая зависимость г) киберкоммуникативная зависимость

**Задание 17**

**Какой Интернет-протокол является безопасным?**

а) ftp:// б) https:// в) http://