Типы вопросов:

multichoice - Множественный выбор/Одиночный выбор

Необходимо выбрать один или несколько правильных ответов

shortanswer - Короткий ответ

Необходимо ввести с клавиатуры правильный ответ

gapselect - Выбор пропущенных слов

Необходимо из выпадающего списка выбрать

matching - Вопрос на соответствие

Необходимо выбрать соответствие элементов друг другу (например, определение и описание)

truefalse - Верно/Неверно

Необходимо выбрать true или false

numerical - Числовой ответ

Необходимо ввести числовой ответ

ordering – Упорядочение

Необходимо выстроить элементы в правильном порядке (например, числа 142 по порядку – 124)

У всех вопросов максимальный балл 1. В свою же очередь ответы на эти вопросы имеют ВЕС – исчисление веса идет в %. Правильный ответ/частичный ответ может принимать вес от 1% до 100% в зависимости от их количества.

Также есть штрафы в некоторых вопросах за выбор неправильного ответа. Например, вы выбрали ответ с весом 50% и один неправильный со штрафом 33% - ваш балл за ответ на вопрос составит 0.12*(УТОЧНЕНИЕ: в минус уйти балл не может, если у вас вес положительных ответов меньше, чем штрафов, то бал равен 0)*

Вопрос 1: Учетные записи в ОС

Тип: multichoice | Максимальный балл: 1

Вася купил новый ноутбук. Он хочет настроить его так, чтобы минимизировать риск заражения системы вирусами при повседневном использовании. Какие из перечисленных действий считаются правилами хорошего тона (best practices) при настройке учетных записей в операционной системе? Выберите все правильные варианты.

A. Всегда работать только под учетной записью «Администратор», чтобы программы запускались без ошибок. (штраф fraction=-33.33333)

B. Создать отдельную учетную запись с правами «Обычный пользователь» для повседневных задач (игры, интернет, учеба). ← правильный/частично верный (fraction=50)

C. Отключить запрос пароля при входе в систему для удобства. (штраф fraction=-33.33333)

D. Установить пароль на учетную запись Администратора. ← правильный/частично верный (fraction=50)

E. Использовать пустой пароль для гостевой учетной записи. (штраф fraction=-33.33333)

Вопрос 2: Безопасность при работе с ОС

Тип: multichoice | Максимальный балл: 1

Вы работаете в компьютерном классе или в библиотеке. Вам нужно срочно отойти на 5 минут. Какие действия обеспечат безопасность вашей сессии в ОС?

A. Выключить монитор кнопкой питания. (штраф fraction=-33.33333)

B. Нажать комбинацию клавиш Win + L (Блокировка экрана). ← правильный/частично верный (fraction=50)

C. Просто свернуть все окна. (штраф fraction=-33.33333)

D. Выйти из системы (Log out), если вы не планируете запускать программы в фоне. ← правильный/частично верный (fraction=50)

E. Повесить на монитор записку «Я скоро вернусь, не трогайте». (штраф fraction=-33.33333)

Вопрос 3: Права доступа к файлам

Тип: ordering | Максимальный балл: 1

Представьте, что в ОС Linux или Windows права доступа записываются тремя группами: для Владельца, для Группы и для Всех остальных Расположите права доступа (разрешения) от наименее безопасного (самого открытого) к наиболее безопасному (строгому) сверху вниз.

Элементы для упорядочивания (правильный порядок):

1) Чтение и запись доступны Владельцу, Группе и Всем остальным.

2) Чтение и запись доступны Владельцу, а Группе и Всем остальным — только чтение.

3) Чтение и запись доступны только Владельцу. Остальным доступ запрещен.

Вопрос 4: Сетевая безопасность ОС

Тип: shortanswer | Максимальный балл: 1

Напишите название компонента операционной системы, который контролирует и фильтрует сетевой трафик, проходящий через компьютер, разрешая или запрещая соединения программ с Интернетом. Он может быть программным или аппаратным. Его часто называют «Межсетевой ...»(компонент имеет несколько вариантов названий в ответе необходимо указать один).

Варианты коротких ответов:

- «*экран*» (fraction=100)

- «*фаервол*» (fraction=100)

- «*брандмауэр*» (fraction=100)

Вопрос 5: Механизм контроля прав

Тип: multichoice | Максимальный балл: 1

В современных версиях Windows, когда вы пытаетесь установить новую программу или изменить важные настройки системы, экран затемняется и появляется всплывающее окно с вопросом: «Разрешить этому приложению вносить изменения на вашем устройстве?» Как называется эта технология защиты?

А. Брандмауэр

B. UAC (User Account Control) ← правильный/частично верный (fraction=100)

C. Режим гибернации

D. Дефрагментация

Вопрос 6: Исправление безопасности ОС

Тип: gapselect | Максимальный балл: 1

Вставьте пропущенные слова в текст, выбрав их из списка (слова могут склоняться).
«Разработчики операционных систем регулярно выпускают исправления безопасности. Это происходит потому, что хакеры постоянно ищут ошибки в коде системы, которые называются [[1]]. Чтобы закрыть такую "дыру" в безопасности, разработчик выпускает [[2]]. Если его вовремя не установить, злоумышленник сможет проникнуть в компьютер, даже если на нем установлен [[3]].»

Сырой текст вопроса (Cloze/пропуски):

> Вставьте пропущенные слова в текст, выбрав их из списка (слова могут склоняться).
> «Разработчики операционных систем регулярно выпускают исправления безопасности. Это происходит потому, что хакеры постоянно ищут ошибки в коде системы, которые называются **УЯЗВИМОСТЬ**. Чтобы закрыть такую "дыру" в безопасности, разработчик выпускает **ПАТЧ (ОБНОВЛЕНИЕ)**. Если его вовремя не установить, злоумышленник сможет проникнуть в компьютер, даже если на нем установлен **АНТИВИРУС**.»

Вопрос 7: Типы вредоносного ПО

Тип: matching | Максимальный балл: 1

Соотнесите название угрозы для операционной системы с её описанием.

Пары для соответствия:

> 1) Троян (Trojan) ↔ Вредоносная программа, которая маскируется под полезное приложение (например, под игру или плеер), чтобы пользователь сам её запустил.
>
> 2) Программа-шифровальщик (Ransomware) ↔ Программа, которая шифрует файлы пользователя и требует деньги за расшифровку.
>
> 3) Кейлоггер (Keylogger) ↔ Программа, которая скрытно записывает нажатия клавиш, чтобы украсть пароли и переписку.

4) Руткит (Rootkit) ↔ Набор программных средств, позволяющий скрыть следы присутствия злоумышленника или вредоносной программы в системе.

Вопрос 8: Режимы ОС

Тип: multichoice | Максимальный балл: 1

Иногда вирус блокирует работу антивируса или не дает удалить себя, постоянно перезапускаясь. В таком случае специалисты рекомендуют загрузить ОС в специальном диагностическом режиме. В этом режиме загружаются только самые необходимые драйверы и компоненты, а программы из автозагрузки (включая вирусы) не стартуют. Как называется этот режим?

A. Режим полета (Airplane Mode)

B. Спящий режим (Sleep Mode)

C. Безопасный режим (Safe Mode) ← правильный/частично верный (fraction=100)

D. Режим инкогнито (Incognito Mode)

Вопрос 9: Восстановление системы

Тип: gapselect | Максимальный балл: 1

Представьте ситуацию: вирус-шифровальщик зашифровал все файлы на компьютере и требует выкуп. Антивирус удалил сам вирус, но файлы остались зашифрованы и открыть их невозможно. Единственный гарантированный способ вернуть свои данные бесплатно в такой ситуации — это восстановить их из [[1]], которая была сделана заранее и хранилась на внешнем диске или в облаке.

Сырой текст вопроса (Cloze/пропуски):

> Представьте ситуацию: вирус-шифровальщик зашифровал все файлы на компьютере и требует выкуп. Антивирус удалил сам вирус, но файлы остались зашифрованы и открыть их невозможно. Единственный гарантированный способ вернуть свои данные бесплатно в такой ситуации — это восстановить их из **РЕЗЕРВНАЯ КОПИЯ**, которая была сделана заранее и хранилась на внешнем диске или в облаке.

Вопрос 10: Устаревшие операционные системы

Тип: multichoice | Максимальный балл: 1

Ваша бабушка использует ноутбук с Windows 7 или Windows XP. Она говорит: «Зачем мне обновлять систему до Windows 10 или 11? У меня стоит хороший антивирус, я в безопасности». Вы, как специалист по безопасности, знаете, что бабушка ошибается. Какая главная причина, почему работать на старых ОС опасно, даже с антивирусом?

A. Старые системы работают медленнее и потребляют больше электричества.

B. У старых систем некрасивый дизайн, который пугает современных хакеров.

C. Разработчик (Microsoft) прекратил поддержку этих ОС: для них больше не выходят исправления (патчи) новых дыр в безопасности. Антивирус не может защитить от уязвимостей в самом «сердце» (ядре) системы. ← правильный/частично верный (fraction=100)

D. На старых системах не запускаются новые игры.

Вопрос 11: Инструменты защиты ОС

Тип: matching | Максимальный балл: 1

У каждого инструмента безопасности своя роль. Соотнесите инструмент с его главной функцией.

Пары для соответствия:

1) Антивирус ↔ Сканирует файлы на диске и в оперативной памяти, сравнивая их с базой известных угроз (сигнатурами).

2) Брандмауэр(Фэервол) ↔ Стоит как стена между компьютером и интернетом, решая, какой программе можно выходить в сеть, а какой — нельзя.

3) VPN ↔ Создает зашифрованный «туннель» для выхода в интернет, скрывая реальный IP-адрес пользователя (полезно в открытых Wi-Fi сетях)

4) Резервное копирование(бэкап) ↔ Копирует важные файлы в «облако» или на внешний диск, чтобы их можно было вернуть в случае поломки или вирусной атаки.

Вопрос 12: Компилируемые языки

Тип: multichoice | Максимальный балл: 1

Выберите компилируемые языки программирования.

A. C ← правильный/частично верный (fraction=20)

B. C++ ← правильный/частично верный (fraction=20)

C. Python (штраф fraction=-30)

D. JavaScript (штраф fraction=-30)

E. PHP (штраф fraction=-30)

F. Go ← правильный/частично верный (fraction=20)

G. Rust ← правильный/частично верный (fraction=20)

H. Pascal ← правильный/частично верный (fraction=20)

Вопрос 13: Memory-unsafe функции в C

Тип: multichoice | Максимальный балл: 1

Какие из перечисленных функций языка C считаются небезопасными с точки зрения работы с памятью?

A. strcpy ← правильный/частично верный (fraction=33.33333)

B. strncpy (штраф fraction=-33.33333)

C. sprintf ← правильный/частично верный (fraction=33.33333)

D. snprintf (штраф fraction=-33.33333)

E. gets ← правильный/частично верный (fraction=33.33333)

F. fgets (штраф fraction=-33.33333)

G. fread (штраф fraction=-33.33333)

H. putc (штраф fraction=-33.33333)

Вопрос 14: Типы PE-файлов

Тип: multichoice | Максимальный балл: 1

Какие типы PE-файлов существуют?

A. .exe ← правильный/частично верный (fraction=33.33333)

B. .docx (штраф fraction=-33.33333)

C. .dll ← правильный/частично верный (fraction=33.33333)

D. .so (штраф fraction=-33.33333)

E. .pdf (штраф fraction=-33.33333)

F. .sys ← правильный/частично верный (fraction=33.33333)

G. .pptx (штраф fraction=-33.33333)

H. .xls (штраф fraction=-33.33333)

Вопрос 15: Соотнести вид ВПО и описание

Тип: matching | Максимальный балл: 1

Соотнесите тип вредоносного ПО с его описанием.

Пары для соответствия:

1) Выдаёт себя за полезное приложение, но выполняет скрытые вредоносные действия. ↔ Троян

2) Скрывает присутствие вредоносных компонентов в системе. ↔ Руткит

3) Самостоятельно распространяется по сети, используя уязвимости. ↔ Червь

Вопрос 16: Название уязвимости

Тип: multichoice | Максимальный балл: 1

На сайте есть форма поиска. Запрос пользователя напрямую подставляется в HTML-страницу без фильтрации. Если в поле поиска ввести строку вроде:
"><h1>TEST</h1>
то при загрузке страницы этот HTML-код будет выполнен браузером и отобразится как часть страницы. Как называется эта уязвимость?

A. SQL Injection

B. Cross-Site Scripting (XSS) ← правильный/частично верный (fraction=100)

C. CSRF

D. Directory Traversal

E. Buffer Overflow

Вопрос 17: Название уязвимости

Тип: multichoice | Максимальный балл: 1

В веб-приложении есть страница загрузки файлов. Пользователь может загрузить изображение, и сервер сохраняет файл под тем же именем, которое указал пользователь. При этом сервер не проверяет, какие именно символы содержатся в имени файла и может сохранить его, например, как:
../../config.txt
В результате злоумышленник получает возможность читать файлы за пределами папки загрузок.
Как называется эта уязвимость?

A. Directory Traversal ← правильный/частично верный (fraction=100)

B. SQL Injection

C. CSRF

D. File Inclusion

E. Use-after-free

Вопрос 18: Соотнесение уязвимостей и описаний

Тип: matching | Максимальный балл: 1

Соотнесите тип веб-уязвимости с её кратким описанием.

Пары для соответствия:

1) Атака, при которой злоумышленник заставляет браузер жертвы выполнить запрос от её имени, например отправить форму без её согласия. ↔ CSRF

2) Внедрение в запрос части SQL-кода для изменения или чтения данных в базе. ↔ SQL Injection

3) Приложение используется как прокси: злоумышленник вынуждает сервер отправлять запросы на внутренние или внешние ресурсы. ↔ SSRF

Вопрос 19: Криптография - основы

Тип: truefalse | Максимальный балл: 1

Цель криптографии - скрыть передачу данных от злоумышленника. В свою очередь, цель стеганографии - не дать ему прочитать содержимое передаваемых данных.

A. true

B. false ← правильный/частично верный (fraction=100)

Вопрос 20: Криптография - комбинаторика

Тип: numerical | Максимальный балл: 1

Вася вводит по одному пин-коду каждые 0.5 секунд (так, что ввод 1 пин-кода занимает 0.5 секунд). В поле ввода пин-кода вводится ровно 4 любых цифры. Вася перебирает коды по порядку, от 0000 до 9999. Он останавливается, когда пин-код оказывается верным. Сколько секунд он потратит в худшем случае?

Числовые ответы:

- **значение 5000** (допуск 0, fraction=100)

Вопрос 21: Криптография - алгоритмы

Тип: multichoice | Максимальный балл: 1

Вы с другом стоите в зале, полном людей. Ваше взаимодействие невозможно скрыть - все, что вы скажите, услышат (другие виды взаимодействия, помимо речи, тоже считаем недоступными). Заранее вы не обменивались никакими ключами/алгоритмами. Как вы можете максимально обезопасить коммуникацию? Никто не должен узнать содержимое ваших разговоров.

A. Воспользоваться симметричным шифрованием для передачи ключа

B. Воспользоваться ассиметричным шифрованием для передачи ключа ← правильный/частично верный (fraction=100)

C. Пробовать случайные ключи, пока они не совпадут

D. Говорить тихо

E. В данной ситуации нельзя обезопасить разговор - в любом случае его прослушают и поймут

Вопрос 22: Криптография - теоретическая безопасность

Тип: multichoice | Максимальный балл: 1

Абсолютно стойкий шифр - это шифр, для которого расшифровать сообщение без ключа принципиально невозможно даже при бесконечных вычислительных ресурсах. Конкретнее, получение зашифрованного сообщения никогда не

дает никакой информации о том сообщении, которое шифровали (кроме заведомо известной). Из перечисленных шифров, ни один не является абсолютно стойким в типичной ситуации. Однако, какие из перечисленных алгоритмов могут стать абсолютно стойкими шифрами при опредленных условиях? Замечание: на сообщение нельзя накладывать никаких ограничений. Не нужно выбирать схемы, которые абсолютно стойки только для сообщений длины 1 и т.п. Однако, размер ключа может адаптироваться под длину шифруемого текста (если длина ключа вообще может меняться в алгоритме), а алгоритм создания ключа, возможно, придется адаптировать особым образом (но он не может зависеть от содержимого сообщения)

A. Шифр Виженера - каждая буква текста заменяется на идущую на k букв позже в алфавите. k равняется номеру соотвествующей буквы ключа. Буквы ключа берутся по порядку и повторяются, если их не хватает. ← правильный/частично верный (fraction=33.33333)

B. Шифр Цезаря - каждая буква текста заменяется на идущую на k букв позже в алфавите. k выбирается заранее, одинаково для всех букв и является ключом. (штраф fraction=-33.33333)

C. AES-ECB - шифрует каждый блок текста из 16 байт при помощи обратимой функции AES. Ключ состоит из 16 байт и определяет поведение функции AES. (штраф fraction=-33.33333)

D. Книжный шифр, где каждый символ текста заменяется на число - номер такого же символа в ключе. Среди множества одинаковых появлений символа в ключе выбирается сначала первое, а затем следующее по номеру, с возвращением к первому в случае отсуствия следующего. (штраф fraction=-33.33333)

E. Шифр подстановки - для каждого возможного текста выбирается шифротекст. Набор этих пар и является ключом. ← правильный/частично верный (fraction=33.33333)

F. Последоватльный полиалфавитный шифр - заранее выбирается публичная последовательность перестановок алфавита, из которых выбирается начальная. По ней заменяется первый символ, по следующей перестановке - второй и т.д. При достижении конца перестановки зацикливаются. Ключ - номер начальной перестановки. ← правильный/частично верный (fraction=33.33333)

Вопрос 23: Сетевая безопасность

Тип: multichoice | Максимальный балл: 1

Николаю в социальной сети пришло сообщение: «Срочно! Твой аккаунт взломали. Чтобы восстановить доступ, перейди по ссылке и введи свой логин и пароль: hack-site.ru». Что следует сделать Николаю??

A. <p class="ds-markdown-paragraph">Немедленно перейти по ссылке и ввести данные, чтобы не потерять аккаунт

B. <p class="ds-markdown-paragraph">Ничего не делать, проигнорировать сообщение. ← правильный/частично верный (fraction=100)

C. <p class="ds-markdown-paragraph">Переслать это сообщение всем своим друзьям, чтобы их предупредить.

D. <p class="ds-markdown-paragraph">Написать в ответ, отправив свой настоящий пароль для проверки.

Вопрос 24: Сетевая безопасность

Тип: multichoice | Максимальный балл: 1

При переходе на сайт онлайн-библиотеки в адресной строке браузера перед адресом появился значок замка и буквы «https». Что это означает?

A. <p class="ds-markdown-paragraph">Сайт точно принадлежит твоему другу.

B. <p class="ds-markdown-paragraph">Соединение с этим сайтом зашифровано, данные передаются в защищённом виде. ← правильный/частично верный (fraction=100)

C. <p class="ds-markdown-paragraph">На этом сайте нельзя ничего купить.

D. <p class="ds-markdown-paragraph">Этот сайт заражён вирусом.