РЕГИОНАЛЬНАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА
ПО ЗАЩИТЕ ИНФОРМАЦИИ
30 ноября 2022 года

СТРУКТУРА ОЛИМПИАДЫ
КЛЮЧЕВЫЕ ТЕМЫ

1. Задание с выбором ответа (2 балла)

Тестовое задание направлено на проверку осведомленности участника в современных тенденциях сферы кибербезопасности:

- Какие угрозы станут ключевыми в ближайшем будущем?
- Какими методами пользуются злоумышленники при совершении атак?
- Как необходимо выстраивать системы управления безопасностью в текущих реалиях?
- Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты?

2. Задание с выбором ответа (2 балла)

Тестовое задание направлено на проверку осведомленности участника в современных тенденциях сферы кибербезопасности:

- Для чего используется симметричное шифрование при построении подсистем безопасности?
- Возможно ли проактивное реагирование на современные кибератаки?
- Совместимы ли open-source решения и информационная безопасность?

3. Обфускация (4 балла)

Не кодом единым. В задании предлагается расшифровать устойчивое выражение, скрытое в синтаксисе известных языков программирования.

Проверим эрудицию?

```
suspend fun hop () = println("cmp 1 1; jmp nxt")
suspend fun say () = println("pog".reversed())
suspend fun main() {
  hop()
  say()
}
```

Ответ: Не говори «гоп», пока не перепрыгнешь.

4. Реагирование на инцидент (6 баллов)

Участникам будет предложено краткое описание инцидента информационной безопасности. Необходимо представить себя в роли «офицера безопасности» и ответить на 2 вопроса:

1) Как этого инцидента можно было избежать?
2) Что нужно было сделать, чтобы минимизировать его последствия?

Для выполнения задания участнику необходимо понимать следующие основополагающие моменты:

- Каким образом выстраивается процесс реагирования на инциденты в системах?
- Каким образом можно этот процесс автоматизировать с использованием средств защиты информации?
- Какие превентивные меры защиты могут помочь не допустить возникновение инцидента?
- Какие основные этапы можно выделить в типовом плане реагирования на инциденты?

5. CTF Win (13 баллов)

Активный пользователь сети приходит с жалобой на замедление работы компьютера. Он проявляет все признаки недовольства: морщит лоб, машет руками — и вообще не собирается долго ждать.

Необходимо найти как можно больше подозрительных и вредоносных объектов на рабочей станции пользователя под управлением **Windows**, проверив типичные места закрепления вредоносных программ.

Каждый участник получает в свое распоряжение виртуальную машину, на которой необходимо найти все подозрительные вредоносные объекты и проверить в каждом из таких объектов наличие скрытого флага. Чем больше таких флагов найдено, тем больше баллов за выполнение задания будет получено.

Флаг в местах закрепления имеет следующий формат:

Flag№1 _ a _ _ _ _ f _

Необходимо записать в пустые клетки отсутствующие символы соответствующего флага.

6. **CTF Lin (18 баллов)**

Все аналогично. Тот же активный пользователь сети, те же претензии и жалобы. Сморщенный лоб и хаотичное движение рук тоже на месте. Вот только рабочая станция теперь под управлением **Debian**.

Необходимо найти как можно больше подозрительных и вредоносных объектов на рабочей станции пользователя под управлением Debian, проверив типичные места закрепления вредоносных программ.

Каждый участник получает в свое распоряжение виртуальную машину, на которой необходимо найти все подозрительные вредоносные объекты и проверить в каждом из таких объектов наличие скрытого флага. Чем больше таких флагов найдено, тем больше баллов за выполнение задания будет получено.

Флаг в местах закрепления имеет следующий формат:

Flag№1 _ w _ _ _ _ h_

Необходимо записать в пустые клетки отсутствующие символы соответствующего флага.

7. **Построение подсистемы безопасности. Участнику будут выданы исходные данные на информационную систему. Необходимо спроектировать подсистему безопасности, руководствуясь требованиями ФСТЭК России о защите информации (25 баллов):**
   1) Провести классификацию информационной системы и определить требования к системе защиты информации **(4 балла)**.
   2) Определить набор средств защиты информации, который сможет реализовать требуемый перечень мер системы защиты информации **(6 баллов)**.
   3) Отобразить на структурно-функциональной схеме места установки выбранных средств защиты информации **(9 баллов)**.

4) Прописать реализацию для мер, которые носят организационный характер **(6 баллов)**.

Результаты выполнения п. 1, 2, 4 отобразить в таблице:

№ п/п	Условное обозначение и номер меры	Реализация меры в системе защиты информации		
		Вид средства защиты информации	Производитель средства защиты информации	Реализация организационными методами
Класс защищенности информационной системы: _____ (указать определенный класс защищенности)				
1.				
2.				
3.				
4.				
5.				
6.				
…	…	…	…	…

Исходные данные ИС «Управление градостроительством»

1.1 Основные сведения об объекте информатизации

1.1.1 ИС «Управление строительством» имеет распределенную клиент-серверную архитектуру.

Серверная часть системы расположена по адресу: 390000, Рязанская область, город Рязань, улица Котовского, дом 4, корпус 2, кабинет № 201, второй этаж.

Клиентская часть состоит из двух типовых АРМ пользователей.

Клиентская часть в составе типовых АРМ пользователей находится по адресам внешних пользователей ИС «Управление градостроительством».

К внешним пользователям ИС «Управление градостроительством»:

– сотрудники казенного учреждения Рязанской области «Центр градостроительного развития Рязанской области»;

– сотрудники государственного автономного учреждения Рязанской области «Центр государственной экспертизы в строительстве Рязанской области»;

– сотрудники органов исполнительной власти Рязанской области и подведомственные им государственные бюджетные учреждения;

– сотрудники местного самоуправления городских округов, органы местного самоуправления городских округов, органы местного самоуправления муниципальных районов Рязанской области.

1.1.2 Границей контролируемой зоны для ИС «Управление градостроительством» являются ограждающие конструкции здания, в котором располагается система в соответствии с п. 1.1.1.

1.1.3 Физический доступ в серверную и кабинеты, где расположены АРМ пользователей, ограничен входным замком, закрывающимся ключом. Список лиц, имеющих доступ в серверную, определен Приказом начальника организации. Список пользователей, имеющих право работы на сервере, определен Приказом начальника организации.

Перечень лиц, которые допущены к обработке конфиденциальной информации на сервере определены приказом начальника организации.

Перечень лиц, которые допущены к обработке конфиденциальной информации на АРМ внешних пользователей определены приказами руководителей, взаимодействующих с ИС «Управление градостроительством» учреждений, органов государственной власти и местного самоуправления.

1.1.4 Функциональная схема ИС «Управление градостроительством» представлена в Приложении А.

1.1.5 Линии электропитания, к которым подключены технические средства ИС «Управление градостроительством», подключены к общегородской электросети. Система заземления соединена с общим контуром заземления здания.

1.2 Сведения об условиях эксплуатации объекта информатизации

1.2.1 ИС «Управление градостроительством» имеет распределенную клиент-серверную архитектуру, в состав которой входит:

1. Сервер гипервизор:
   а) аппаратного обеспечения:
      1) физический сервер;
   б) ПО:
      1) аппаратный гипервизор «VMware ESXi»;
2. Сервер базы данных, функционирующий на базе:
   а) аппаратного обеспечения:
      1) сервер гипервизор;
   б) ПО:
      2) операционная система «Debian»;
      3) СУБД «PostgreSQL»;
3. Сервер приложений, функционирующий на базе:
   а) аппаратного обеспечения:
      1) сервер гипервизор;
   б) ПО:
      1) операционная система «Debian»;
      2) сервер приложений «Mojolicious»;
      3) HTTP сервер «Nginx»;

4) клиент протокола SSL OpenSSL;

4. Сервер картографии, функционирующий на базе:

а) аппаратного обеспечения:

1) сервер гипервизор;

б) ПО:

1) операционная система «Debian»;
2) компонент «MapServer»;
3) «QGis» сервер;

5. Сервер хранилище, функционирующий на базе:

а) аппаратного обеспечения:

1) физический сервер;

б) ПО:

1) операционная система «Debian»;

6. Клиентская часть типового АРМ пользователя № 1, функционирующая на базе:

а) аппаратного обеспечения:

1) системный блок;
2) монитор;
3) клавиатура;
4) манипулятор «Мышь»;

б) ПО:

1) лицензионная операционная система «Windows 10 Pro»;
2) пакет офисных программ «Мой офис»;
3) браузер «Yandex»;

7. Клиентская часть типового АРМ пользователя № 2, функционирующая на базе:

а) аппаратного обеспечения:

1) системный блок;
2) монитор;
3) клавиатура;

4) манипулятор «Мышь»;

б) ПО:

1) лицензионная операционная система «Astra Linux Special Edition 1.6»;

2) пакет офисных программ «LibreOffice»;

3) браузер «Mozilla Firefox»;

Для ИС «Управление градостроительством» объектами защиты являются сведения в области градостроительной деятельности, программно-технический комплекс системы.

1.2.2 ИС «Управление градостроительством» работает круглосуточно для обеспечения возможности своевременного межведомственного информационного взаимодействия с внешними системами и регламентированного представления сведений о документах ИС «Управление градостроительством» через веб-интерфейс.

1.3 Сведения об информации, обрабатываемой в системе

1.3.1 В ИС «Управление градостроительством» обрабатывается информация, не содержащая сведения, составляющие государственную тайну. В соответствии с функциональными возможностями подсистем ИС «Управление градостроительством», обрабатывается следующая информация:

– информация о градостроительной деятельности;

– заявления о предоставлении сведений, содержащихся в ИС «Управление градостроительством»;

– реестр и карточки документов;

– квитанции (счета) на оплату за оказание государственной услуги по предоставлению сведений, содержащихся в ИС «Управление градостроительством»;

– справки о предоставлении сведений, содержащихся в ИС «Управление градостроительством»;

– регистрационные данные документов;

– общие показатели документов;

– отчетные данные по предоставлению услуг по выдаче сведений из ИС «Управление градостроительством»;

– дела о застроенных и подлежащих застройке земельных участков;

– документы территориального планирования.

ИС «Управление градостроительством» функционирует на территории субъекта Российской Федерации и имеет сегменты в нескольких муниципальных образованиях и подведомственных и иных организациях.

ИС «Управление градостроительством» создана во исполнение Постановления Правительства Рязанской области «Об обеспечении устойчивого функционирования градостроительной деятельности Рязанской области».

Для свойств безопасности защищаемой информации в ИС определены следующие степени ущерба:

– конфиденциальность: низкая степень;

– целостность: низкая степень;

– доступность: низкая степень.

Структурная схема ИС «Управление градостроительством»