

УТВЕРЖДЕНО  
Приказом ГБУ ДО «ДЮТТ  
Челябинской области»  
от «24» февраля 2022 г. № 35

**ПОЛОЖЕНИЕ**  
**о проведении**  
**IT-квеста «Кибербезопасность»**

Челябинск

2022

# IT-квест «Кибербезопасность»

Основная задача Квеста - осуществить переход в закрытый паролем секретный раздел суперважного сайта. Ссылка на сайт в файле. Файл в закрытом паролем архиве. Архив в ноутбуке. Вход в учетную запись ноутбука закрыт паролем.

Предыстория такова. Есть вымышленная организация, занимающаяся торговлей неким товаром. В организации достаточно стандартный набор персонала: директор, главный бухгалтер, системный администратор, менеджеры и уборщица. Участники квеста - команда злоумышленников, к которым совершенно случайно попадает один из ноутбуков одного из менеджеров организации. На этом ноутбуке есть ценный для команды взломщиков ресурс, к которому необходимо получить доступ. Хакерам заранее не известны ни пароли, ни какому из менеджеров организации принадлежит ноутбук. Команда вправе использовать любые средства для достижения главной цели - доступа к нужной информации: программные средства, методы социальной инженерии. Не допускается физическое вмешательство в архитектуру ноутбука (разбирать ноутбук нельзя). Команды могут обмениваться между собой ценной информацией и игровой валютой для достижения целей. Переход участников из одной команды в другую во время прохождения квеста запрещен.

## Система начисления очков

За успешное выполнение квеста команды получают следующее количество очков:

1-е место (на решение задачи затрачено наименьшее время) - 100 очков

2-е место (второе время) - 90 очков

3-е место - 80 очков

...

9-е место - 10 очков

10-е место - 0 очков.

Презентация решения судейской бригаде может принести дополнительные очки от 0 до 20 (решение о начислении дополнительных очков принимается судейской бригадой коллегиально)

## Требования к паролям

Пароль на вход в учетную запись ноутбука - сложный

Пароль на архив - 12345

Пароль на секретный раздел сайта - сложный, но прямо прописан в исходном файле страницы

## Сотрудники организации - жертвы

Каждый сотрудник в нашей организации имеет свой уникальный характер, должность, степень осведомленности и степень влияния на других сотрудников организации. Как и в любой реальной организации, отношения внутри коллектива сложные и не всегда

очевидные. Изначально участники команд точно знают о должностях каждого сотрудника и могут попасть на прием к любому сотруднику (в порядке очереди), другая информация о характерах персонажей до участников не доводится, участникам придется выяснить это самостоятельно.

**Директор.** Слабо понимает, чем занят персонально каждый из менеджеров, часто путает имена менеджеров, но требует от менеджеров одного - продажи товара. Обычно действует через главного бухгалтера. Мало что понимает в методах социальной инженерии, компьютерах. На встрече с участниками команд может очень долго рассуждать на различные темы, прямо не отвечая на вопросы участников (тянуть время). После продолжительной дискуссии может дать ответ о личных предпочтениях одного из менеджеров (подсказку на приобретение в магазине товаров), но не уточняет имя менеджера. Не знает ни одного пароля и не сильно паникует на тему информационной безопасности. Подарки берет с удовольствием, в ответ дарит только товар и передает просьбы главному бухгалтеру. На столе среди кучи сторонних документов могут лежать резюме сотрудников с намеками на хобби, увлечения.

**Главный бухгалтер.** Всегда очень занят. Знает, какому менеджеру какой ноутбук принадлежит. Не знает ни одного пароля. Принимает указания от директора, но не всегда их исполняет, а если исполняет, то чаще всего с ошибками. На любые вопросы от участников команд, связанных с компьютерной техникой отсылает к системному администратору и заканчивает беседу. Вообще не разбирается в информационной безопасности, на столе масса бумаг с явными простыми паролями, но среди них ни одного нужного. Подарки принимает, а после получения подарка выполняет поручение директора качественно (если такое поручение поступило от директора). Готов за половину цены выкупить товар, но только если его об этом попросят.

**Системный администратор.** Крайне неразговорчив, в организации совсем недавно. Знает, какому менеджеру какой ноутбук принадлежит. Знает все пароли. На любые вопросы, связанные с компьютерами и сотрудниками отвечает только сотрудникам организации, но, т.к. работает недавно, то не всех сотрудников помнит. Знает все о компьютерной безопасности, на прямые вопросы, связанные с информационной безопасностью реагирует максимально агрессивно и прекращает общение. Подарки принимает от всех, но реагирует на них исключительно нытьем о тяжелой жизни айтишника. С гостями готов поговорить на любую тему, связанную с информационными технологиями и может продать "чудо-флешку для взлома любого пароля", которая на самом деле ничего полезного не содержит. Назад флешку принимает неохотно и за половину стоимости. На столе куча ненужного мусора, в том числе та самая флешка.

**Менеджеры.** Общие свойства всех менеджеров нашей организации:

Болтливые люди, сначала пытающиеся продать товар, но в любом разговоре постоянно скатывающиеся на тему своей специализации (хобби). Знают только свой ноутбук и только свои пароли. Любой ноутбук считают своим. У каждого на столе бумаги, среди которых две подсказки, ведущих к паролям. Кроме бумаг на столе подсказки, указывающие на специализацию (хобби) менеджера. Знают и любят посплетничать о специализации всех менеджеров. Средний уровень познаний в

области информационной безопасности, панику поднимают только на прямой вопрос о паролях. Выполняют поручения главного бухгалтера. Пароли озвучивают только посторонним и только после грамотного запроса со стороны участников (социальная инженерия). Чем больше подарков получают менеджеры или чем больше товара продают, тем охотнее верят в методы социальной инженерии.

Специализация (шестой символ в ответе команды совпадает с номером команды):

### **Менеджер 1 Спортсмен**

Пароль на Windows: "Трактор"

Дополнительные вопросы/ответы:

-В каком городе родились? Тамбов

-Ваше прозвище в детстве Верзила

-Имя старшего двоюродного брата или сестры Семен

Пароль на архив: "4NcbV8GEWw"

Подарки: мяч, медаль

### **Менеджер 2 Поэт**

Пароль на Windows: "Ямб"

Дополнительные вопросы/ответы:

-В каком городе родились? Москва

-Ваше прозвище в детстве Стихоплет

-Имя старшего двоюродного брата или сестры Игорь

Пароль на архив: "schTeDBVHv"

Подарки: книга, ручка

### **Менеджер 3 Летчик**

Пароль на Windows: "Пилотирование"

Дополнительные вопросы/ответы:

-Мое самое страстное увлечение? Пилотирование

Пароль на архив: "dHkQvQoAPx"

Подарки: самолетик, очки защитные

### **Менеджер 4 Программист**

Пароль на Windows: "EasyHome"

Дополнительные вопросы/ответы:

-Моя первая программа EasyHome

Пароль на архив: "fMaJjroDnj"

Подарки: клавиатура, провод

### **Менеджер 5 Автолюбитель**

Пароль на Windows: "АвтоВАЗ"

Дополнительные вопросы/ответы:

-То, с чем готов проводить время часами АвтоВАЗ

Пароль на архив: "Zsjim3qEts"

Подарки: гаечный ключ, тряпка

### **Менеджер 6 Строитель**

Пароль на Windows: "Строительство"

Дополнительные вопросы/ответы:

-Что вдохновляло в детстве Строительство

Пароль на архив: "CsLmbeq3ga"

Подарки: молоток, плоскогубцы

#### **Менеджер 7 Любитель поездов**

Пароль на Windows: "Ласточка"

Дополнительные вопросы/ответы:

-Что нравилось больше всего Ласточка

Пароль на архив: "VAdeez4BsD"

Подарки: чайный пакет, конфета

#### **Менеджер 8 Химик**

Пароль на Windows: "Оксид водорода"

Дополнительные вопросы/ответы:

-Моя первая формула Оксид водорода

Пароль на архив: "yPDIByEfMS"

Подарки: белый порошок, ампула с химикалиями

#### **Менеджер 9 Повар**

Пароль на Windows: "Пельмешки"

Дополнительные вопросы/ответы:

-В каком городе родились? Пермь

-Ваше прозвище в детстве Повар

-Имя старшего двоюродного брата или сестры Катя

Пароль на архив: "h2t6GK1ErU"

Подарки: ложка, салфетка

#### **Менеджер 10 Критик**

Пароль на Windows: "Кино"

Дополнительные вопросы/ответы:

-Чем заинтересовался в первом классе Кино

Пароль на архив: "dqZO1Y3KCK"

Подарки: фотография, маркер

**Уборщица.** Знает все о всех менеджерах (хобби, любимые подарки) и с удовольствием делится этой информацией с любыми посетителями совершенно даром. Не знает ничего о информационной безопасности, не знает что такое ноутбук. Знает, но забыла любой пароль. Пароли пытается долго вспомнить, но так ничего и не вспоминает. Подарки принимает, но кроме обильных благодарностей ни к чему не влекут. Попытки вернуть подарок со стороны участника вызывает в уборщице гнев и панику.

## Подсказки

Несколько подсказок, способных помочь участникам в прохождении Квеста.

- Основной принцип: “Я люблю клубнику. Я люблю ловить рыбу. Но если рыбу я буду кормить клубникой, то не поймаю ни одной. Рыбу надо кормить тем, что она любит, – червями. Если ты хочешь стать другом кому-то, – не говори о клубнике, которую ты любишь. Говори о червяках, которых любит он.”
- Обращайте внимание на лежащие на столе предметы, они могут содержать в себе подсказки (а могут и не содержать);
- Каждый Менеджер организации имеет свой определенный характер, стиль жизни или хобби (спортсмен, театрал, начинающий программист и т.п.), воспользуйтесь этими знаниями;
- Никогда не действуйте напрямую, социальные инженеры никогда так не поступают.

## Команда.

Каждая команда состоит из 7 участников. Каждый участник имеет определенную роль и определенные функциональные возможности. Роли распределяются внутри команды самостоятельно, но не допускается передача роли от одного участника команды другому на всем протяжении Квеста. Все члены команды могут участвовать в обсуждении тактических и стратегических приемов, направленных на прохождение Квеста.

### Роли:

1. **Капитан команды.** Общая координация работы команды, выбор стратегии, принятие тактических решений. Решающее слово при возникновении споров внутри команды принимает капитан команды. Презентация истории взлома судейской бригаде после прохождения Квеста.
2. **Хакер.** Единственный член команды, которому разрешена работа с ноутбуком-жертвой. Именно этот человек вводит пароли, занимается поиском нужных папок и файлов.
3. **Коммуникатор 1.** Коммуникаторы ведут переговоры с сотрудниками организации - жертвы. Другие участники команды к общению с сотрудниками не допускаются. Следуют стратегии, выбранной капитаном команды. Основная задача коммуникаторов - при помощи методов социальной инженерии узнать необходимую информацию у сотрудников организации - жертвы.
4. **Коммуникатор 2.** Аналогично п.3
5. **Финансист.** Отвечает за условную игровую валюту, совершает покупки в магазине приманок. Учитывает все возможные траты, не допускает отрицательного баланса бюджета команды.
6. **Разведчик.** Ведет переговоры с разведчиками других команд на предмет обмена ценной информации на информацию или игровую валюту. Не допускаются силовые методы добычи информации у команд-соперников. Допускаются любые договоренности между разведчиками команд, такие договоренности обязаны соблюдаться. При несоблюдении договоренностей

капитан команды в праве подать жалобу ведущему, но обязан предоставить доказательства договоренности.

7. **Блогер.** Пишет историю взлома, тщательно фиксируя каждый сделанный шаг, принятое решение, расход игровой валюты и прочие шаги квеста. Приветствуется литературное оформление истории взлома. История взлома презентуется судейской бригаде после прохождения квеста. Блогер должен иметь собственный смартфон (планшет / ноутбук) с возможностью подключения к сети Wi-Fi и аккаунт в Google для оформления блога (ссылка на файл блога предоставляется организаторами в виде QR-кода перед началом Квеста).

#### **Деньги.**

Изначальный капитал у каждой команды: 150 квантиков.

Цена каждого предмета в магазине 50 квантиков.

Магазин товар назад не принимает. Команды ведут товарообмен самостоятельно (устанавливают цены, принимают решения о продаже и т.п.)

#### **Подготовка:**

- деньги купюры по 25 квантиков x 60шт.
- подсказки для сотрудников
- таблички с должностями на стол
- таблички с номерами команд
- прайс-лист магазина
- бейджи для каждого участника команды (с описанием роли)
- на каждую команду QR-код с доступом на google-документ (история успеха)
- собрать товар в магазин