Проектирование и стохастический анализ системы безопасности

Описание

Рассматривается некоторая информационная система **A**. Пользователи этой системы могут реализовывать различные варианты поведения, среди которых выделим класс *потенциально опасных действий*[1]:

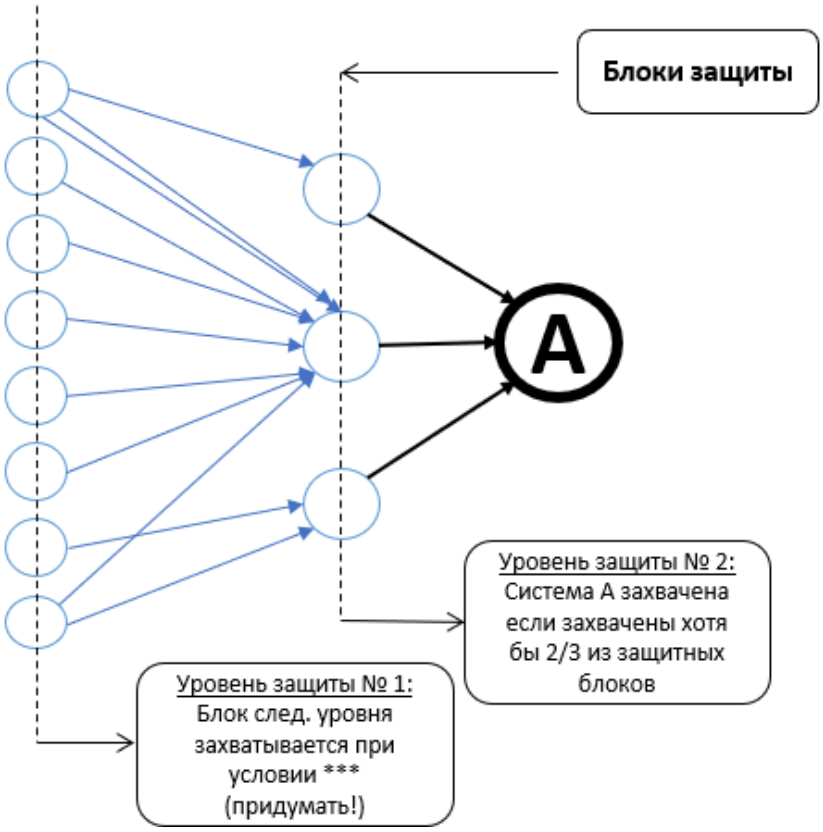
1' Просмотр кода страниц;
2' Частое просматривание личных данных других пользователей;
3' Массовые рассылки другим пользователям;
4' И т. д.[2]

Помимо потенциально опасных для системы действий со стороны пользователя, он обладает возможностью реализации n различных действий и не ограничен в количестве реализации этих действий.

Для обеспечения безопасности функционирования системы **A** требуется разработать систему безопасности **B**, которая могла бы анализировать действия пользователей системы **A** с целью заблаговременного обнаружения потенциальных угроз.

Задание

Представьте проект системы B изобразив ее в виде графа с уровнями защиты не менее двух. Пример:



[1] Действия, которые **могут быть** направлены на перехват управления системой или несанкционированный сбор данных о ее функционировании.
[2] Предложенные варианты действий можно заменить и дополнить – на усмотрение команды.

Каждая команда сама определяет, что из себя представляют уровни защиты и варианты их прохождения таким образом, чтобы каждое действие в системе могло быть реализовано как «мирным» пользователем, так и злоумышленником. Например, первый уровень защиты представляет собой вход в аккаунт пользователя. Некто (обозначим его за X) пытается войти в систему заявляя, что он забыл пароль. Для доступа к аккаунту, система направляет X проверочный цифровой пароль по смс. Считается, что если X злоумышленник, то он всегда точно вводит полученный пароль – в случае, если у него есть доступ к телефону пользователя, а если X мирный, то он, получив смс с цифровым паролем просто пытается его запомнить, при этом вероятность ввода каждой последующей цифры по памяти определяется каким-либо образом (может распределением задается)!

Цель

- составить проект системы безопасности с несколькими уровнями защиты;
- представить его иллюстрацию, схему;
- охарактеризовать / описать каждый уровень защиты;
- задать на каждом уровне защиты (или вершине) условие прохождения пользователя в след. уровень, а также условие, при выполнении которого пользователь будет подозреваться как злоумышленник и в доступе к системе ему будет отказано;
- важно!!!: считается, что если доступ к системе слишком сложный, неудобный или часто требует повторной авторизации и т.д., то пользователь перестает пользоваться системой и уходит. А это очень плохо!
- описать в докладе проекта вероятность взлома системы (она должна быть положительной) согласно придуманным уровням защиты и тех действий, что в них заложены;
- учесть возможности для повышения или снижения уровня защиты под различные уровни терпения пользователей. Составить не менее 3-х вариантов уровня терпения пользователя (например, пользователи готовы во время использования системы пройти повторную авторизацию не более одного раза и т. п.) и продемонстрировать как для каждого случая меняется вероятность взлома.

Примечание к результатам.

Необходимо использовать разделы курса, которые были до случайных величин. Важно стремиться найти баланс между сложностью защиты и удовлетворенностью пользователей с плохой памятью и творящих всякое, чтоб их не потерять. То есть все хотят максимальной защиты, но хотят при этом, чтобы все было легко и просто! **Поэтому каждая команда может презентовать свой проект-продукт!**