УДК 004.056

РАЗРАБОТКА ТРЕБОВАНИЙ ДЛЯ ВЕБ-ИНТЕРФЕЙСОВ СИСТЕМ КОНТРОЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Дибиров Г.М. (Санкт-Петербургский государственный университет телекоммуникаций им. профессора М. А. Бонч-Бруевича)

Научный руководитель – кандидат технических наук, доцент Ковцур М.М.
(Санкт-Петербургский государственный университет телекоммуникаций им. профессора М. А. Бонч-Бруевича)

Научный руководитель – кандидат технических наук, доцент Бабков И.Н.
(Санкт-Петербургский государственный университет телекоммуникаций им. профессора М. А. Бонч-Бруевича)

Аннотация

В этом докладе формулируются требования, учитываемые при разработке веб-интерфейсов систем контроля информационной безопасности. Рассмотрены возможные уязвимости и методы защиты от них, а также наиболее важные компоненты интерфейса.

Введение.

При работе с сетями связи и информационными системами пользователи сталкиваются с важной задачей — обеспечение информационной безопасности сетей и систем. Для решения данной задачи используются различные системы контроля информационной безопасности, позволяющие полноценно контролировать работу сети, её пользователей, анализировать трафик, искать злоумышленников. Для корректной работы подобных систем нужно также придерживаться некоторых требований при создании их веб-интерфейсов. В существующей литературе не удалось обнаружить источники, описывающие требования для современных интерфейсов систем контроля информационной безопасности. При этом в условиях импортозамещения и активной разработки отечественного программного обеспечения формализация таких требований является актуальной задачей.

Основная часть.

Довольно частой уязвимостью в различных система управления информационной безопасностью может являться нарушенный контроль доступа. Подобная уязвимость может привести к следующему сценарию. Пользователь обходит разграничение прав, к примеру, с помощью изменения параметров в get-запросе или же перебора типовых названий страниц. Таким образом, он может получить доступ к файлам страниц других пользователей или суперпользователей. Последствием таких действий может стать полный сбой рабочей системы.

Предлагается использовать несколько методов решения данной проблемы. Можно использовать разные модели доменов, таким образом, строго разграничивая доступ пользователей с одними правами на одном домене, других, соответственно, на другом домене.

Также необходимо внедрить повторное подтверждение пароля пользователя при совершении действий, оказывающих влияние на всю систему в целом. Важно, чтобы при этом не было возможности проведения межсайтового скриптинга, с последующей генерацией всплывающего окна, требующего подтверждения пароля. Для этого следует правильно выбирать фреймворки, с помощью которых строится веб-интерфейс

К тому же не стоит забывать об аннулировании переменных сессии и токенов JWT (JSON WebToken) на сервере после выхода из системы. Это позволяет обезопасить каждый новый сеанс пользователя.

Вспомогательным решением для устранения данной уязвимости можно назвать регистрацию сбоев контроля доступа и уведомление главного администратора при необходимости.

Стоит отметить, чтобы система могла обеспечивать безопасность, пользователю данной системы нужно вовремя и точно оценить параметры и данные сети. Для этого необходимо, обеспечить интерфейс удобным меню, предоставляющим доступ к страницам: с основными параметрам устройств внутри сети, с настройками политик безопасности, вывода и обработки событий в сети и т.п. Немаловажно, чтобы на главной странице веб-интерфейса были размещены дашборды с диаграммами для отображения основных статистических данных, отражающих состояние информационной системы.

Таким образом, можно сформулировать следующие требования для веб-интерфейсов систем контроля информационной безопасности:

- применение разных моделей доменов;
- повторное введение пароля;
- аннулирование JWT токенов,
- регистрация сбоев контроля доступа,
- наглядное и удобное меню с дашбордами.

Остальные требования разобраны в докладе.

Выводы.

В данной работе были предложены некоторые требования, учитывая которые можно получить безопасный и наглядный веб-интерфейс системы контроля информационной безопасности. Эти требования могут быть внедрены в различную техническую документацию или в политики информационной безопасности организации-разработчика подобных систем контроля.

Дибиров Г.М. (автор)	Подпись
Ковцур М.М. (научный руководитель)	Подпись
Бабков И.Н. (научный руководитель)	Подпись