

Литература

1. Hacking the Skills Shortage. A study of the international shortage in cybersecurity skills [Electronic resource]. Mode of access: <https://www.mcafee.com/ca/resources/reports/rp-hacking-skills-shortage.pdf>. Date of access: 14.05.2017.
2. Sheridan, K. 7 Cyber-Security Skills In High Demand [Electronic resource]. Mode of access: <http://www.informationweek.com/strategic-cio/security-and-risk-strategy/7-cyber-security-skills-in-high-demand-/d-id/1326494>. Date of access: 14.05.2017.
3. Information Security Analyst Skills [Electronic resource]. Mode of access: <https://www.thebalance.com/information-security-analyst-skills-2062409>. Date of access: 14.05.2017.
4. Лыньков, Л.М. Методика оценки рисков информационной безопасности в системах электронной экономики / Л.М. Лыньков, Т.Н. Беляцкая, В. С. Князькова // Доклады БГУИР. – 2017. – № 2 (104). – С. 69–76.

ЗАЩИТА ИНФОРМАЦИИ В МОБИЛЬНОМ ПРИЛОЖЕНИИ «МЕНЕДЖЕР ПЕРИОДИЧЕСКИХ ПЛАТЕЖЕЙ»

А.В. Бердник, А.В. Матвеев

Объектом защиты информации в рассматриваемом докладе является мобильное приложение «Менеджер периодических платежей». В настоящее время все чаще необходимо использовать периодические платежи, такие как оплата телефона, учебы или услуг ЖКХ. Некоторые платежные системы в нашей стране позволяют настроить автоматические платежи на некоторые услуги, однако функционал регулирования частоты оплаты, как правило, отсутствует, и в целом данный способ не всегда уместен либо пугает некоторых пользователей из-за отсутствия личного контроля за платежами. Приложение подразумевает использование различных платежных систем, в том числе и использование системы расчета ЕРИП (Единое Расчетное и Информационное Пространство) [1]. Система ЕРИП имеет возможность выставления счета на некоторые услуги (оплата учебы, некоторых услуг ЖКХ и так далее), следовательно, зная идентификатор пользователя в данной услуге, приложение может само получить необходимую сумму к оплате. При создании событий пользователь может указать поведение программы в данном случае: предлагать полученную сумму, не оплачивать в случае если суммы нет или игнорировать данные ЕРИП и оплатить сумму, указанную пользователем.

Приложение работает с реальными деньгами пользователя, следовательно, каждое его одобрение оплаты должно быть подтверждено введением личного пароля. Пользователь может установить пароль при регистрации, которая запускается при первом запуске программы. Уникальным ключом каждого пользователя является номер мобильного телефона, изменить его можно в настройках программы. Пользователь может подключать к программе несколько платежных карт различных банков или платежных систем, либо другие способы оплаты (интернет-кошелек, оплата со счета мобильного) и в будущем, при создании событий, сможет выбрать с помощью какого способа оплаты оформить услугу. Также возможно выбирать способ оплаты перед каждым непосредственным платежом. Работа с платежными системами и системой расчета ЕРИП накладывает на приложение большую ответственность за информационную безопасность данных пользователя и всех проводимых операций. Опыт показывает, что простого пароля для авторизации в системе недостаточно, необходима шифровка данных при любых синхронизациях с сервером приложения и наличие безопасного соединения при отправке команд в систему расчета.

Литература

1. ЕРИП Расчет – Платежные агенты [Электронный ресурс]. – Режим доступа: <http://raschet.by/bankam/platezhnye-agenty/>. – Дата доступа: 19.05.2017.

ОСОБЕННОСТИ АНКЕТИРОВАНИЯ СОТРУДНИКОВ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ ПРИ ПРОВЕДЕНИИ АУДИТА СИСТЕМЫ МЕНЕДЖМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Бойправ, Л.Л. Утин, В.В. Ковалёв

Предложен перечень вопросов для анкетирования сотрудников организаций электросвязи в зависимости от специфики деятельности последних: строительство