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/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-кошельки, 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

(организации категории 1), предоставление услуг электросвязи (организации категории 2), проектирование сетей электросвязи (организации категории 3), управление и регулирование деятельности организаций электросвязи (организации категории 4). Вопросы составлены с учетом требований к системе защиты информации, изложенных в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62, а также положений СТБ ISO/IEC 27001-2016.

Сотрудники, которых следует отнести к кругу лиц, подлежащих опросу в ходе аудита системы менеджмента защиты информации организаций электросвязи: руководитель и/или главный инженер; начальник службы безопасности; старшие производители работ или начальники строительных участков (в случае, если аудируемая организация относится к категории 1); начальники отделов, сотрудники которых работают с электронными документами и базами данных, в которых содержится информация ограниченного распространения (в случае, если аудируемая организация относится к категории 2, 3 или 4).

Из составленных авторами статьи анкетных вопросов для руководителей и/или главных инженеров организаций электросвязи категорий 1–4 можно выделить следующие основные:

1. Выполнена ли классификация КВОИ, доступ к которым имеют сотрудники Вашей организации? 2. Выполняется ли в Вашей организации классификация активов КВОИ, доступ к которым имеют сотрудники? 3. Внедрена и используется ли в Вашей организации политика информационной безопасности? 4. Назначено ли в Вашей организации лицо, на которое возложены обязанности по контролю за соблюдением положений политики информационной безопасности? 5. Осведомляются ли увольняемые сотрудники Вашей организации, которые имели доступ к информации ограниченного распространения, об ответственности, к которой они могут быть привлечены вследствие разглашения этой информации третьим лицам?

СИСТЕМА МОНИТОРИНГА И КОРРЕЛЯЦИЙ СОБЫТИЙ

Ю.О. Быханьков

Для построения эффективной системы защиты информации не только следует разобраться в требованиях законодательства, но и соизмерить их с финансовыми возможностями организации, а также определить механизм мониторинга и аудита информационной безопасности. На текущий момент в Республике Беларусь необходимость в системе мониторинга и корреляций событий следует из регулирующих приказов Оперативно-аналитического центра при Президенте Республики Беларусь и действующих, но местами неработающих и даже противоречащих законодательству стандартов серии 34.101. В виду того что требования к системе защиты информации закреплены, иногда возможно изменить класс объекта информатизации (информационной системы), чтобы уменьшить затраты на построение системы защиты информации, например сокращением средств на реализацию требований пп. 39, 40, 46 приказа № 62 ОАЦ, а в некоторых случаях на разработку и оценку задания по безопасности. Требования по сбору, просмотру и анализу событий безопасности являются обязательными в Республике Беларусь для систем защиты информации независимо от формы собственности. Уменьшение средств защиты может не только навредить безопасности, но и помочь, сфокусировав внимание специалиста. В списке сертифицированных средств уже существуют продукты для адекватного исполнения требований по анализу событий, в то же время существуют варианты формального выполнения пунктов требований регулятора, которые не могут сравниться с системами корреляций событий. В том же приказе прописывается анализ событий уполномоченными субъектами, однако как показывают исследования, квалифицированные субъекты без специальных средств не могут выполнять анализ на должном уровне в режиме реального времени, особенно анализ логов с различных элементов инфраструктуры, что является критически важным для обеспечения защиты информации.

Литература

1. Закон Республики Беларусь Об информации, информатизации и защите информации от 10 ноября 2008 г. № 455-З.

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62.