практическое применение в деятельности руководства и персонала конкретного предприятия, на котором планируются и проводятся мероприятия по обеспечению ИБ объектов информационной инфраструктуры. Недостаточная подготовка персонала организации, слабое знание им нормативно-правовой базы по вопросам обеспечения безопасности может стать причиной уязвимостями эксплуатируемых информационных систем. Применение организационных методов обеспечения ИБ является обязательной составляющей обеспечения ИБ любой организации.

Организационно-правовая база обеспечения ИБ разрабатывается и описывается при проектировании и создании, а также последующей аттестации СЗИ информационной системы предприятия. Государственное предприятие «НИИ ТЗИ» является одной из ведущих организаций Республики Беларусь в области защиты информации. Вот уже более четверти века одним из направлений деятельности государственного предприятия «НИИ ТЗИ» является проектирование и создание СЗИ, предназначенных для решения задач защиты информации в самых разных информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено и не отнесенной к государственным секретам, а также аттестации таких систем в соответствии с действующим законодательством Республики Беларусь.

В докладе подробно представлены основные этапы разработки и формирования документации, регламентирующей организационные методы обеспечения ИБ и сопровождающей СЗИ информационной системы предприятия на всех этапах ее проектирования, создания и аттестации.

НАВЫКИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.Н. Беляцкая, В.С. Князькова

По оценкам специалистов, к 2019 г. в мире будет не заполнено от 1 до 2 миллионов вакансий в сфере информационной безопасности (ИБ). Например, в 2015 г. в США было свободно около 209000 вакансий в сфере ИБ. Такая нехватка специалистов может быть причиной сдерживания развития электронного общества, в частности, электронной экономики. Исследование, проведенное компанией Intel Security, показало, что 82% всех респондентов (страны: Австралия, Франция, Германия, Израиль, Япония, Мексика, Великобритания и США) указали на нехватку знаний в области ИБ. Это напрямую приводит к экономическим затратам у 71 % респондентов, главным образом из-за большей уязвимости организаций перед хакерскими атаками, а также в связи с необходимостью оплачивать труд специалистов в сфере ИБ более высоко. Так, в указанных выше странах заработная плата специалиста в области ИБ в 2,7 раза выше средней по отрасли.

Выделяют следующие основные навыки, которыми должен обладать специалист области ИБ. Во-первых, аналитические (способность к изучению компьютерных систем, оценке потенциального риска и способность предложить возможное решение). Во-вторых, коммуникационные (специалист в области ИБ должен обучать пользователей, объясняя им важность ИБ и способы защиты персональной и коммерческой информации). В-третьих, креативность (необходимо предугадывать действия компьютерных преступников, что требует нестандартного мышления). В-четвертых, внимательность к деталям (зачастую угрозы ИБ трудно распознать, поэтому специалист в области ИБ должен отслеживать даже незначительные изменения в информационной системе, предвидя любые, даже несущественные, потенциальные проблемы). В-пятых, знания в IT сфере (и угрозы, и методы их предотвращения постоянно меняются, поэтому необходимо постоянно совершенствовать свои знания по последним решениям, законодательству, практиками и методикам в области защиты информации). В качестве основных элементов образовательной системы в области ИБ рассматривается классическое академическое образование; при этом его интеграция с практической компонентой лучше подготовит будущего специалиста. Для оценки качества подготовки специалистов в сфере ИБ, Intel Security разработала интегрированный показатель, учитывающий расходы на образование; программы по науке, технологиям, инженерии и математике; наличие дисциплин по ИБ в вузах; использование передовых практик. Наилучшие результаты достигнуты такими странами, как США и Великобритания.

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