DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3
УДК 332(075.8)
ББК 65.422

БЕЗОПАСНОСТЬ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ

Сергей Иванович Кравченко

Старший преподаватель кафедры «Информационная безопасность»,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
nikita.lgov@mail.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

Аннотация. В данной статье рассмотрена проблема обеспечения информационной безопасности социотехнических систем при разработке онлайн-приложений. Описывается структура социотехнической системы, ее подсистемы и этапы обеспечения безопасности такой системы. Кроме того, рассматривается применение социотехнического подхода, его преимущества и недостатки.

Ключевые слова: информационная безопасность, социотехническая система, политика безопасности, оценка ущерба.

Основной целью данной статьи является краткое изложение концепции организации информационной безопасности социотехнических систем (ИБ СТС) при разработке онлайн-приложений в части, касающейся непосредственно защиты обрабатываемой информации. В системах данного типа огромную роль играет защита информации, учитывающая как социальные, так и технические аспекты. В статье рассматриваются теоретические вопросы, связанные с обеспечением ИБ СТС в рамках онлайн-обслуживания клиентов. Представленная в работе структура ИБ СТС направлена на создание системы, которая совмещает в себе удобство эксплуатации и надежную защиту информации [4]. В ее модель также заложена возможность непрерывных оптимизации и совершенствования для повышения эффективности эксплуатации пользователями. Цель представленной структуры – обратить внимание разработчиков онлайн-приложений на возможный способ защиты информации путем включения в систему компонентов, учитывающих поведение пользователей.

Для начала рассмотрим, что включает в себя понятие «социотехническая система».

Социотехническая система (СТС) представляет собой рабочую систему, состоящую из технической подсистемы, подсистемы персонала и внешней среды, взаимодействующей с организацией [1]. В общем контексте информационной безопасности организация безопасности СТС включает в себя два этапа. Первый – применение технических возможностей системы без учета поведения пользователя; второй – применение технических возможностей системы с учетом характеристик поведения пользователя. Таким образом, в составе СТС можно выделить две подсистемы: техническую и социальную. Это подчеркивает важность технических аспектов социально-технического подхода, поскольку основная его цель – создать систему, которая отвечает техническим задачам и позволяет пользователям эффективно использовать систему.

Рассмотрим подробнее работу этих подсистем.

Техническая подсистема представляет собой совокупность программного обеспечения, аппаратных устройств, методов, конфигураций и процедур, применяемых пользователями системы для преобразования входных данных в выходные.

Социальная подсистема включает в свой состав людей и организации, которые взаимодействуют с системой. При этом неизбежно проявляются их уникальные социальные признаки. Социальная подсистема в организации должна рассматриваться не как набор отдельных свойств, а как их взаимосвязанная общность. Такая система будет обладать признаками интегративности свойств.

При разработке СТС необходимо учитывать модель системы [2], предназначенную для объединения пользователей в группы с одинаковыми правами.

Создание политики безопасности на основе модели доступа пользователей к защищаемой информации является важным шагом, оказывающим большое влияние на ИБ СТС. Сначала необходимо определить несколько контрольных групп, созданных для разграничения пользователей и их действий относительно объектов, к которым они имеют доступ. При этом пользователи, имеющие доступ к различным уровням защищаемой информации, могут относиться к одинаковым группам, то есть при обладании одинаковыми правами в отношении политики доступа они могут различаться в окончательном наборе возможностей осуществления операции чтения, модификации (вплоть до подмены) и удаления элементов из набора критичных документов.

Для обеспечения защиты обрабатываемых данных вводится модель информационного объекта, обладающая рядом параметров, среди которых можно выделить: идентификационные данные объекта, оценку ущерба при потере конфиденциальности, целостности и доступности.

Последние три атрибута позволяют дать оценку критичности причиненного ущерба организации, который возникает при несанкционированном доступе к защищаемой информации. Для снижения риска возникновения подобных ситуаций чаще всего достаточно соотносить все производимые операции с идентификаторами пользователей и вовремя реагировать на все подозрительные действия.

Таблица «Идентификатор пользователя» состоит из:

– персонального идентификатора и имени группы пользователя;

– описания групп пользователей;

– наделения пользователей правами доступа (разрешения типа «Чтение», «Запись» и «Удаление»);

– областей и объектов хранения защищаемой информации.

В качестве потенциальных нарушителей рассматриваются: зарегистрированные пользователи СТС; разработчики программного обеспечения; лица, случайно или умышленно получившие доступ к информационной системе (хакеры).

Существуют следующие предположения о характере возможных действий нарушителей:

– несанкционированные действия пользователей могут быть следствием наличия уязвимостей программного обеспечения, а также недостатков технологии обработки, хранения и передачи информации;

– в своей деятельности потенциальный нарушитель может использовать любое имеющееся средство несанкционированного съема и перехвата информации, воздействия на информацию и информационные системы, а также другие средства и методы для достижения стоящих перед ним целей;

– нарушитель может быть в сговоре с разработчиком системы.

Необходимость использования социотехнических подходов еще более важна в системах, связанных с информационной безопасностью. Информационные системы могут быть криптографически защищенными благодаря современным механизмам шифрования. При этом существует риск потерпеть неудачу, если пользователи неправильно используют или обходят их. Социальные атаки, такие как социальная инженерия, делают криптографическую защиту бесполезной. Учитывая все нюансы, создание надежной системы безопасности становится сложной задачей по причине сильной связи с человеческим фактором. Это обуславливает необходимость применения социотехнического подхода. Примером последнего является создание интерактивных систем безо-

пасности, в которых для эффективной эксплуатации конечного продукта разработчикам необходимо обеспечить баланс между информационной безопасностью и удобством работы с информационными системами. Социотехнический подход также применим для решения вопросов защиты информации онлайн-приложений. Благодаря его использованию можно получить продукт, который является одновременно и полезным, и безопасным.

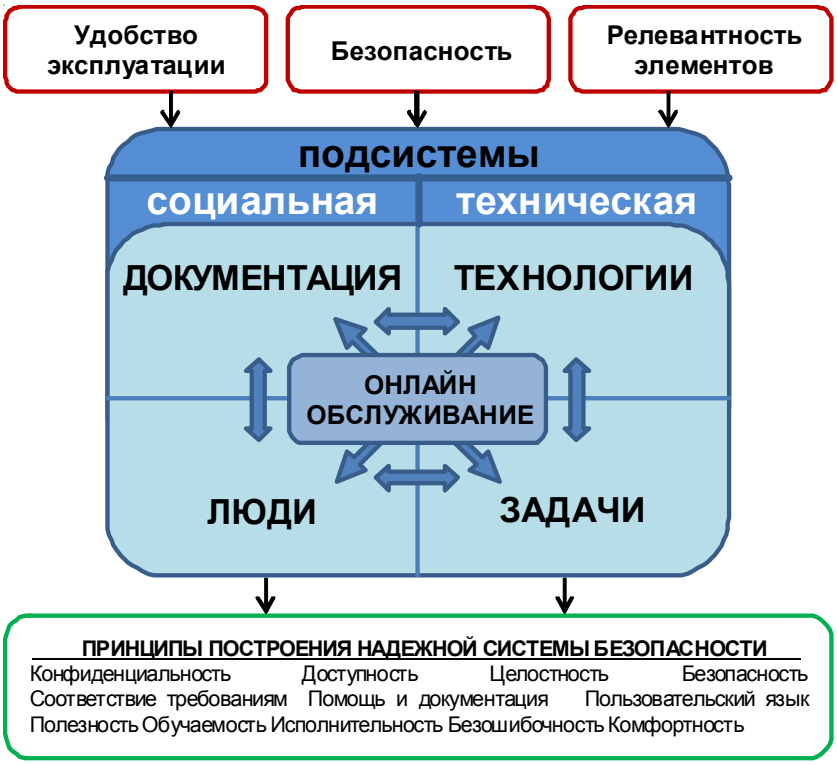
Наглядным примером организации безопасности социотехнических систем является разработка онлайн-приложений, создатели которых стремятся реализовать эффективную систему безопасности, соответствующую всем необходимым требованиям. Создается среда, которая способствует принятию и продолжению использования приложений различными пользователями. Это определение относится к онлайн-банковским системам, но может применяться к любым другим онлайн-приложениям, требующим организации межсетевой безопасности.

На рисунке 1 изображены компоненты СТС, к которым относятся и внешние факторы, влияющие на систему. Схема отражает соответствие требованиям безопасности и комфортности использования продукта, необходимым для надежной и стабильной работы системы. Используя оценку релевантности компонентов системы, с высокой точностью можно определить восприятие пользователями текущей услуги. Эта оценка основана на отзывах пользователей и позволяет выделять области, которые требуют особого внимания для улучшения обслуживания.

Рассмотрим назначение и порядок функционирования представленных на рисунке компонентов СТС, а также основные требования к ним [3].

Удобство эксплуатации необходимо для обеспечения рационального и продуктивного пользования системой и оказывает существенное влияние на привлечение новых клиентов. Очень важно, чтобы система соответствовала данному требованию в начале ее построения, так как ее организация на более позднем этапе может сопровождаться значительными трудностями. Приложения, работающие с информационными системами, должны обеспечивать надежную защиту предоставленной пользователями конфиденциальной информации.

Требование к обеспечению безопасности особенно важно, когда риск может привес-



Структура организации информационной безопасности социотехнических систем

ти к финансовым убыткам или утечке конфиденциальной информации клиентов. Примером является система дистанционного банковского обслуживания. Следовательно, при разработке системы необходимо учитывать механизмы обеспечения безопасности для защиты личной информации пользователей.

Немаловажной является релевантность элементов системы.

Для того чтобы пользователи стали доверять онлайн-приложениям, созданным для дистанционного банковского обслуживания, требуются не только полезность и простота использования. Необходимо, чтобы пользователи имели обратную связь с разработчиками. Это помогает создавать системы, соответствующие таким требованиям, как удобство пользования, безопасность, конфиденциальность, доступность и др.

Организационно-правовые документы необходимы для того, чтобы создать организацию, соответствующую всем требованиям, установить ее структуру, функции структурных подразделений, осуществить организацию труда и распределение обязанностей между работниками, определить порядок взаимодействия с клиентами и перечень применяемых норм и стандартов.

Нормативно-правовые документы устанавливают рекомендуемое поведение для пользователей, а также обязанности и обязательства в отношении предоставляемых им услуг. Эти положения и условия включают процедуры разрешения споров в случаях нарушения безопасности или возникновения других проблем. Документация также включает в себя проектные подходы, используемые при разработке системы, в частности применение местных и международных стандартов и передовых методов, которые являются обязательными или рекомендуемыми при разработке приложений (или продуктов). Стандарты могут включать в себя те из них, которые предусмотрены международными органами, такими как International Organisation for Standardisation (ISO).

К лицам, участвующим в системе дистанционного обслуживания, относят пользователей, разработчиков, руководство организации и любые другие заинтересованные стороны.

Пользователи – это клиенты сервиса, которые представляют собой группу людей разного возраста, образования, уровня компьютерной грамотности, национальности и культуры. Разработчики – это всеобъемлющий термин. К ним относятся дизайнеры, программисты, тестировщики, оценщики удобности интерфейса, поставщики аутсорсинговых продуктов и любые другие люди, непосредственно участвующие в разработке онлайн-приложений. Руководство включает в себя высшее начальство учреждения.

К технологиям относят широкий спектр компонентов, являющихся частью системы дистанционного обслуживания: от аппаратных и пользовательских устройств до программных приложений, которые предоставляют услуги. Со стороны организации технологии охватывают аппаратные серверы, операционные системы, сетевые технологии между центрами обработки данных, платформы промежуточного программного обеспечения, серверные приложения и пользовательские интерфейсы, которые позволяют сотрудникам и пользователям получать доступ к информации удаленно. Организация также предоставляет технологии и механизмы обеспечения информационной безопасности, чтобы защитить пользователя и активы компании. Эти технологии включают в себя шифрование, брандмауэры, а также системы обнаружения и предотвращения вторжений.

Изложенный в статье материал раскрывает подход, направленный на повышение эффективности в разработке онлайн-приложений с помощью использования социотехнического метода. Благодаря применению обратной связи с пользователями удается в значительной степени улучшать существующие системы, а также уменьшить риск отказа пользователей от эксплуатации удаленными системами, связанный с отсутствием удобства эксплуатации и недостаточно надежной защитой их персональных данных.

Для достижения этой цели должны быть идентифицированы факторы, которые влияют на поведение пользователя, а также препятствуют ему производить нежелательные действия.

Создание системы защиты информации в онлайн-приложениях должно способствовать нейтрализации факторов, побуждающих пользователей применять средства, направленные на обход или игнорирование механизмов защиты информации. Следовательно, применение социотехнического подхода при разра-

ботке систем защиты информации будет способствовать достижению цели создания безопасных и пригодных для использования приложений, а рассмотренная структура ИБ СТС является механизмом для их реализации.

СПИСОК ЛИТЕРАТУРЫ

1. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах : учеб. пособие для вузов / Г. А. Остапенко, Е. А. Мешкова ; под общ. ред. В. Г. Кулакова. – М. : Горячая Линия-Телеком, 2016. – С. 1–3.

2. Тулупьев, А. Л. Информационная модель пользователя, находящегося под угрозой социоинженерной атаки / А. Л. Тулупьев, А. А. Азаров, А. Е. Пащенко // Труды СПИИРАН. – 2010. – Вып. 2 (13). – С. 143–155.

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – М. : ИД «ФОРУМ» : ИНФРА-М, 2011. – 416 с.

4. Mujinga, M. A Socio-Technical Approach to Information Security / M. Mujinga, M. M. Eloff, J. H. Kroeze // AMCIS. – 2017. – P. 1–8.

REFERENCES

1.Ostapenko G.A., Meshkova E.A. *Informatsionnye operatsii i ataki v sotsiotekhnicheskikh sistemakh* [Information Operations and Attacks in the Socio-Technical Systems]. Moscow, Goryachaya Liniya-Telekom Publ., 2016, pp. 1-3.

2. Tulupyev A.L., Azarov A.A., Informatsionnaya model polzovatelya, nakhodyashchegosya pod ugrozoy sotsioinzhenernoy ataki [Information model of the user under threat of social engineering attack]. *Trudy SPIIRAN*, 2010, iss. 2 (13), pp. 143-155.

3. Shangin V.F. *Informatsionnaya bezopasnost kompyuternykh sistem i setey* [Information security of computer systems and networks]. Moscow, FORUM; INFRA-M Publ., 2011. 416 p.

4.Mujinga M. , Eloff M.M., Kroeze J.H. A Socio-Technical Approach to Information Security. *AMCIS*, 2017, pp. 1-8.

THE SECURITY OF SOCIO-TECHNICAL SYSTEMS

Sergey I. Kravchenko

Senior Lecturer, Department of Information Security,
South-Russian State Polytechnic University named after M.I. Platov
max_wanted@mail.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

Abstract. The paper deals with the problem of information security of socio-technical systems when developing online applications. The structure of the socio-technical system, its subsystems and the stages of protection the information of such a system are described. The application of the socio-technical approach, its advantages and disadvantages are also studied.

The material presented in the paper reveals the approach aimed at improving the efficiency in the development of online applications through the use of social engineering method. The positive factor is the use of feedback by users able to significantly improve existing systems, to reduce the risk of failure of the user from the operation of the remote systems associated with the lack of ease of use and unreliable protection of their personal data.

To achieve this goal, we should identify the factors that affect the user's behavior, as well as prevent users from performing unwanted actions.

The creation of an information security system in online applications should help to neutralize the factors that encourage users to use tools to bypass or ignore information security mechanisms. Therefore, the use of social engineering approach in the development of information security systems will contribute to the goal of creating safe and usable applications.

Key words: information security, socio-technical system, security policy, damage assessment.