References

1. Alagic J., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Yi-Kai Liu., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.* Available at: http://dx.doi.org/10.6028/NIST.IR.8240.

2. Baan H., Bhattacharya S., Fluhrer S., Garcia-Morchon1 O., Laarhoven T., Player R., Rietman1 R., Saarinen M.-J. O., Tolhuizen1 L., Torre-Arce J. L., Zhang Z. Round5: KEM and PKE based on (Ring) Learning with Rounding. *National Institute of Standards and Technology.* Available at: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions.

3. Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. Report on Post-Quantum Cryptography. *National Institute of Standards and Technology.* Available at: https://doi.org/10.6028/NIST.IR.8105.

4. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking. *National Institute of Standards and Technology.* Available at: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf.

5. *Nist software perfomance tests.* Available at: https://www.safecrypto.eu/pqclounge/round-1-candidates/software-analysis-kem/.

6. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 1997, vol. 26, no. 5, pp 1484–1509.

7. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process. Available at: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

DOI 10.21672/2074-1707.2019.48.4.127-135
УДК 004.01

РАЗРАБОТКА МОДЕЛИ УГРОЗ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С УЧЕТОМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Статья поступила в редакцию 13.11.2019, в окончательном варианте – 25 11.2019.

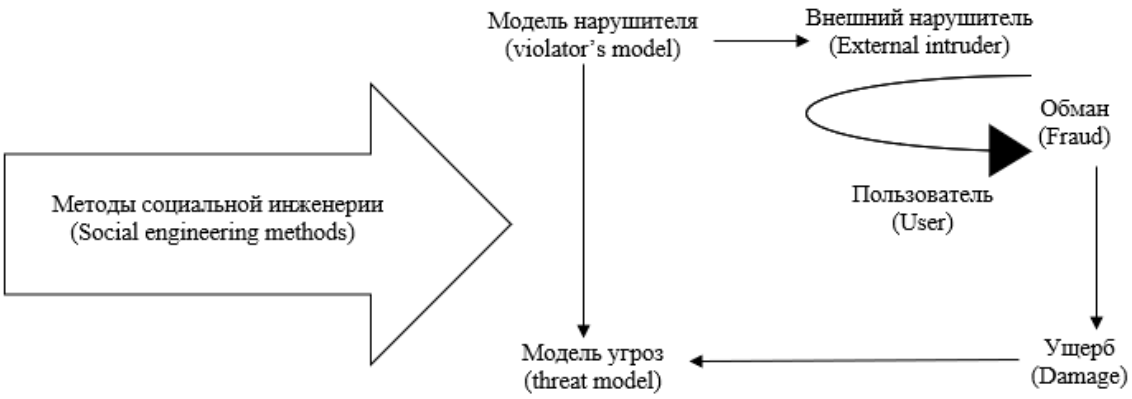
Новикова Елизавета Федоровна, Кубанский государственный университет, 350072, Российская федерация, г. Краснодар, ул. Московская, д. 2,
аспирант, e-mail: lizanovicova@mail.ru

Хализев Вячеслав Николаевич, Кубанский государственный университет, 350072, Российская федерация, г. Краснодар, ул. Московская, д. 2,
кандидат технических наук, профессор e-mail: ha53@mail.ru

Рассмотрен новый подход к разработке модели угроз безопасности информации объектов критической информационной инфраструктуры (КИИ). Значимость настоящей работы обуславливается увеличением компьютеризации населения, что повышает вероятность возникновения угроз от использования методов социальной инженерии. Вследствие отсутствия до конца проработанной нормативной и методической базы в области безопасности объектов КИИ в работе используется как основа обязательная к реализации «классическая» методика ФСТЭК формирования модели угроз безопасности информации. Данная модель расширяется компонентами, учитывающими человеческий фактор, который отсутствует в «классической» методике. В статье выделены виды нарушителей, которые могут использовать методы социальной инженерии, а также непосредственно сопоставлены нарушители и реализуемые ими методы. Приводятся возможные деревья угроз и атак. Результаты данного исследования являются основой для программной реализации системы моделирования угроз и выработки мер противодействия.

Ключевые слова: критическая информационная инфраструктура, категорирование, объект критической информационной инфраструктуры, модель потенциального нарушителя, модель угроз безопасности информации, человеческий фактор, социальная инженерия

Графическая аннотация (Graphical annotation)



THE DEVELOPMENT OF A THREAT MODEL FOR CRITICAL INFORMATION INFRASTRUCTURE FACILITIES CONSIDERING SOCIAL ENGINEERING METHODS

The article was received by the editorial board on 13.11.2019, in the final version –25.11.2019.

Novikova Elizaveta F., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
post-graduate student, e-mail: lizanovicova@mail.ru
Khalizev Vyacheslav N., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Professor, e-mail: ha53@mail.ru

A new approach to the development of an information threat model of critical information infrastructure objects is considered. The significance of this work is determined by the increasing computerization of the population, which increases the likelihood of threats from the use of social engineering methods. Due to the lack of a fully developed regulatory and methodological base in the field of security of CII objects, the work uses the "classical" FSTEC methodology to create a mandatory model of information security threats. This model is expanded by components that take into account the human factor, which is absent in the "classical" methodology. The article defines the types of violators who can use the social engineering methods, as well as directly correlates the violators and the methods that they implement. Possible trees of threats and attacks are given. The results of this study are the basis for the software implementation of an information threat model and the development of countermeasures.

Key words: critical information infrastructure, categorization, object of critical information infrastructure, violator's model, information threat model, human factor, social engineering

Введение. 1 января 2018 г. вступил в силу Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [10], который регулирует отношения в области обеспечения безопасности объектов КИИ в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак. Принятие данного закона стало новым этапом в развитии законодательства в области информационной безопасности [1].

Несмотря на то, что Федеральный закон № 187-ФЗ был принят почти два года назад, многие законодательные и методические «дырки», связанные с безопасностью объектов критической информационной инфраструктуры, так и остаются «незакрытыми».

Литературу, связанную с безопасностью объектов КИИ, в настоящее время целесообразно разделить на два периода: опубликованные до 1 января 2018 г. и после. Это разделение связано с устареванием или неактуальностью информации, содержащейся в них. Так, объекты КИИ ранее рассматривались в рамках законодательства, связанного с безопасностью АСУ ТП. Для подтверждения этого приведем в качестве примера [2], в котором в разделе 2 рассматривается «модель нарушителя» и «модель угроз для АСУ ТП».

Литература, являющаяся частью «нового» периода вследствие малого времени от вступления в силу Федерального закона № 187-ФЗ, немногочисленна и из-за отсутствия до конца проработанной нормативной базы в большинстве случаев носит характер аналитических обзоров.

Так, в статье [1] приведен обзор структуры органов государственной власти в области обеспечения безопасности объектов КИИ.

В работе [3] дан аналитический обзор подходов к идентификации объектов КИИ, который отражен в документе [12]. Также [3] отражает подход, используемый на территории Российской Федерации; поднимает вопрос категорирования объектов КИИ. В данной статье впервые автором поднимается вопрос о расширении модели угроз безопасности информации человеческим фактором. В качестве объекта рассмотрения он выбран не случайно. Сегодня человек, «управляющий» информационной системой, зачастую может не «успеть» за бесконечно развивающимся информационно-техническим миром. Эмоции, неопытность, наивное поведение иногда становятся уязвимостями, через которые возможна реализация угроз безопасности КИИ, что может повлечь за собой потери. Примером может быть схема взлома по телефону, когда при звонке нарушитель входит в доверие к жертве, представляясь, например, сотрудником банка.

О методах социальной инженерии есть упоминание в методическом документе [7]. В нем определено, что одна из угроз безопасности информации может быть реализована нарушителями за счет воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Приведем определения некоторых терминов.

Фишинг – метод социальной инженерии, целью которого является получение конфиденциальных данных пользователей – логина и пароля. Примером такой схемы является отправка сообщений, содержащих ссылки на фальшивые веб-страницы. Троянский конь – атака, при которой также осуществляется сбор конфиденциальной информации, однако при реализации схемы фишинга атака происходит на стороннем ресурсе, а троянского коня – утечка идет с автоматизированного рабочего места (АРМ) пользователя.

Претекстинг – метод социальной инженерии, в рамках которого нарушитель выдает себя за лицо, являющееся доверенным лицом по отношению к жертве.

Кви про кво – метод социальной инженерии, при реализации которого злоумышленник использует контактный телефон или корпоративную почту. Целью атаки является получение информации при оказании «помощи», например, подставным оператором технической поддержки.

Обратная социальная инженерия – атака, направленная на создание злоумышленником условий, при которых жертва сама обращается к нарушителю.

Анализ существующих источников по разработке «модели нарушителя и угроз объектов КИИ» отражает их «незаконченность» при отсутствии угроз безопасности от методов социальной инженерии.

Использование схем фишинга, претекстинга, кви про кво, троянского коня, обратной социальной инженерии могут нанести большой урон существующим системам [11].

Таким образом, актуальной задачей является разработка модели угроз безопасности информации, расширенной человеческим фактором, а именно, защитой объектов от атак, использующих методы социальной инженерии.

Постановка задачи. Целью данной работы является введение учета человеческого фактора, а именно защиты от атак, использующих методы социальной инженерии, в модель угроз безопасности информации.

Основной задачей является непосредственно разработка методики для формирования модели угроз безопасности информации.

Методы. Любая информационная система должна быть включена в документ «Модель угроз и нарушителя». Задача на первый взгляд кажется легкой, но в условиях некоторой методической неопределенности осуществить это может быть трудно.

С одной стороны, когда нет методической базы, можно использовать какой-либо стандартный шаблон, согласно которому непосредственно разрабатывать требуемое. Пример: модели угроз и нарушителя для информационной системы персональных данных (ИСПДн) и государственной информационной системы (ГИС) имеют похожую структуру. Следовательно, для объектов КИИ модель угроз и нарушителя будет отличаться только в характерных, свойственных объекту КИИ отношениях.

С другой стороны, при отсутствии методической базы, проверяющий из организации-регулятора может видеть «правду» по-другому, что станет причиной изменений внутренних документов организации и дополнительных перепроверок.

Если представить, что субъективизма проверяющего нет, то остается некий «шаблон», который к тому же является в своем роде стандартным, что значит универсальным.

При разработке «Модели угроз и нарушителя» можно ориентироваться как на действующие методики («Базовая модель угроз безопасности персональных данных при их обработке в инфор-

мационных системах персональных данных» [5], «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [6], «Меры защиты информации в государственных информационных системах» [4]), так и на проекты методик («Методика определения угроз безопасности информации в информационных системах» [7]).

При выполнении разработки начальным этапом каждой модели угроз и нарушителя является детальное описание каждого объекта КИИ, формирующее перечень защищаемых ресурсов. Данное описание должно иметь «правдивый» характер и включать в себя следующее:

- описание непосредственно организации, владеющей или арендующей объект КИИ;
- описание информационной системы (ИС), определяющее точное назначение и состав данных объектов КИИ в организации и показывающее схемы потоков защищаемой информации, а также отражающее перечень и состав обрабатываемой информации;
- таблицы допуска пользователей к ресурсам;
- схему локально-вычислительной сети (ЛВС) организации.

Вышеперечисленные пункты помогают выявить более широкий перечень угроз безопасности объектов КИИ.

Далее следует выполнить категорирование объектов КИИ, опираясь на методы, закрепленные законодательно [8, 9].

На следующем этапе следует обратиться к «классической» модели: перед субъектом КИИ стоит задача классификации, или же, ориентируясь на существующее законодательство, категорирование объектов КИИ. Так, «Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [8] определяет 14 пунктов. Согласно им требуется провести экспертную оценку, т.е. в некотором роде определить субъективную оценку в соответствии с социальной, политической, экономической, экологической значимостью, значимостью для обеспечения обороны страны, безопасности страны и правопорядка. Субъективизм зависит только от мнения эксперта.

Определение категории объекта КИИ дает основание для разработки «Модели потенциального нарушителя», где в соответствии все с теми же методиками определяется актуальность, возможности и потенциал для всех типов нарушителей.

Если ориентироваться на Методику [7], то наиболее вероятными нарушителями, использующими методы социальной инженерии, являются специальные службы иностранных государств (блоков государств), внешние субъекты (физические лица), конкурирующие организации, преступные группы (криминальные структуры), администраторы информационной системы и администраторы безопасности. В первом случае нарушителя интересуют наиболее значимые объекты государства, при этом целью является получение лидерства на мировой арене в экономике, политике, медицине, оборонно-промышленном комплексе.

Внешний субъект всегда будет актуальным в отношении к объекту КИИ, потому что интерес получить доступ к чему-то запрещенному не угасает никогда в людях.

Физические лица могут как целенаправленно, так и бесцельно стремиться к взлому, нарушению; использовать зачастую методы социальной инженерии.

Конкурирующие организации преследуют цель установления лидерства в какой-либо отрасли как на территории одного региона или государства, так и в случае наличия возможностей для этого – на территории нескольких государств. Для конкурирующих организаций методы социальной инженерии – один из основных способов добывания информации.

Преступные группы, администраторы ИС и администраторы безопасности своей целью могут ставить выявление уязвимостей, а также сбор информации, представляющей собой коммерческую или государственную тайну, для их продажи и получения выгоды.

Следует также учитывать, что существует конкурентная разведка, при реализации которой могут использоваться методы социальной инженерии, но в рамках действующего законодательства.

Подведение итогов. Использование «Модели потенциального нарушителя» может служить основой для разработки «Модели угроз безопасности информации» объектов КИИ.

На данном этапе в соответствии с архитектурой инфраструктуры выделяются объекты воздействия. В данном случае субъекты, кстати, тоже являются объектом воздействия [7]. Если задуматься, то «физическое устранение», например, администратора ИС, который единственный в организации знал все ключи и пароли, может привести к нарушению функционирования объекта КИИ в случае его выключения [3].

Таблица 1 – Виды нарушителей, использующих методы социальной инженерии

Вид нарушителя	Описание
Специальные службы иностранных государств (блоков государств)	Тип нарушителя: внешний, внутренний. Потенциал нарушителя: высокий. Методы социальной инженерии: фишинг, троянский конь, кви про кво.
Внешние субъекты (физические лица)	Тип нарушителя: внешний. Потенциал нарушителя: низкий. Методы социальной инженерии: фишинг, троянский конь, претекстинг, кви про кво.
Конкурирующие организации	Тип нарушителя: внешний. Потенциал нарушителя: средний. Методы социальной инженерии: фишинг, троянский конь, претекстинг, кви про кво.
Преступные группы (криминальные структуры)	Тип нарушителя: внешний. Потенциал нарушителя: средний. Методы социальной инженерии: фишинг, троянский конь, претекстинг, кви про кво.
Администраторы информационной системы и администраторы безопасности	Тип нарушителя: внутренний. Потенциал нарушителя: средний. Методы социальной инженерии: претекстинг.

Ссылаясь на вышесказанное, можно составить дерево атак, одна из ветвей которой представлена на рисунке 1.

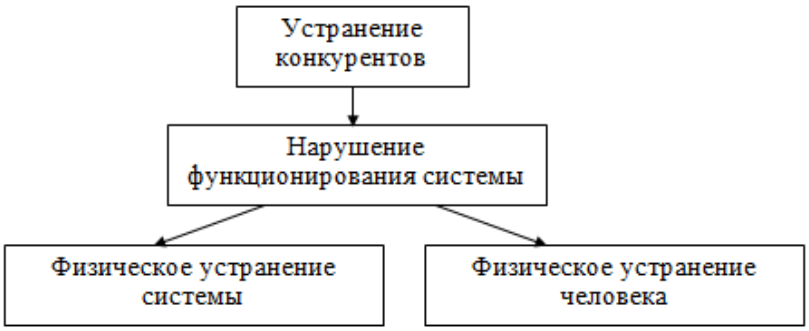


Рисунок 1 – Дерево атак

Под «физическим устранением системы» понимается нарушение функционирования объекта КИИ, «физическим устранением человека» – невозможность ответственного сотрудника находиться на рабочем месте с полным отсутствием связи с ним.

Дерево угроз, если рассматривать его с позиций классификации на естественные и искусственные угрозы, всегда содержит в «искусственной» ветви человеческий фактор, так как именно человек является зачастую главной угрозой вследствие своих эмоциональных и поведенческих характеристик: любопытство, зависть, неопытность и т.д. (рис. 2).

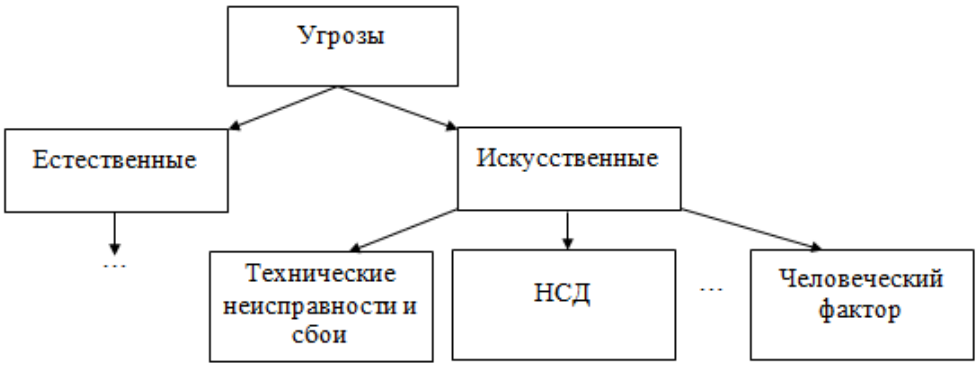


Рисунок 2 – Дерево угроз

Несмотря на наличие человеческого фактора в дереве угроз, в «Модель угроз безопасности информации» он не попадает. И новым в данном исследовании является факт самого внесения человеческого фактора, т.е. в данном случае отход от «стандартного» шаблона.

На основании этого «Модель угроз безопасности информации» будет иметь расширенный вид за счет введения в нее угроз от реализации методов социальной инженерии.

Результаты. Результатом данного исследования является подготовка полной теоретической базы для реализации программного комплекса (ПК) по разработке «модели нарушителя и угроз» объектов КИИ. При написании ПК будут использованы базы данных. Выходными данными ПК станет пакет документов по объектам КИИ: акт категорирования объектов КИИ, перечень объектов КИИ, заключение о формировании перечня объектов КИИ, приказ об ответственности за обеспечение безопасности объектов КИИ, приказ о создании комиссии по категорированию объектов КИИ, уведомление ФСТЭК России о результатах категорирования объектов КИИ, модель нарушителя и угроз объектов КИИ. При этом реализуемая модель не будет противоречить действующим нормативным документам, а лишь дополнять их.

Категорирование объектов критической информационной инфраструктуры. В соответствии с п. 6 «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации» [8] объекту КИИ по результатам категорирования присваивается категория с наивысшим значением или не присваивается вовсе, если ни один из показателей не применим к данному объекту:

$$K = max(K_j),$$

где K_j – показатель.

Разработка модели угроз безопасности информации. Независимо от характера угрозы любая из них должна быть рассмотрена отдельно. Показатель актуальности угрозы безопасности:

$$\text{УБИ}_j^A = [P_j;\ X_j],$$

где P_j – вероятность или возможность реализации угрозы; X_j – степень ущерба.

Вероятность или возможность реализации угрозы:

$$P_j = [K; Y],$$

где K – категория; Y – потенциал нарушителя.

Исходя из заданных параметров, можно составить таблицу, отражающую вероятность (возможность) реализации угрозы безопасности информации нарушителем на объект КИИ (табл. 2).

Таблица 2 – Вероятность (возможность) реализации угрозы безопасности информации нарушителем на объект КИИ

Потенциал нарушителя	**Категория объекта КИИ**		
	3	2	1
Низкий	Низкая	Средняя	Высокая
Средний	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

Степень возможного ущерба объекта КИИ при реализации угрозы безопасности может быть высокой, средней и низкой. В первом случае нарушение одного из свойств безопасности информации может привести к существенным негативным последствиям для субъекта КИИ, в последнем случае – возможны незначительные последствия негативного характера. Знание вероятности (возможности) реализации угрозы безопасности информации нарушителем на объект КИИ и степени возможного ущерба позволяет определить актуальность угрозы безопасности информации (табл. 3).

Таблица 3 – Определение актуальности угрозы безопасности информации

Вероятность (возможность) реализации угрозы	**Степень возможного ущерба**		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

Построение системы защиты информации на основе данной модели должно перекрывать как угрозы, подходящие под определение человеческого фактора, так и любую другую угрозу, реализуемую при помощи технических или организационных мер (табл. 4).

Таблица 4 – Построение системы защиты информации для объекта КИИ с учетом возможностей использования нарушителями методов социальной инженерии

Метод социальной инженерии, используемый нарушителем	**Меры борьбы**
Фишинг	Обучение пользователей ИС правилам использования ресурсов интернета; ознакомление их с политикой конфиденциальности; использование антивирусного программного обеспечения (АВПО), использование межсетевых экранов (МЭ)
Троянский конь	Ознакомление с политикой конфиденциальности, использование АВПО, использование МЭ
Претекстинг	Ознакомление с политикой конфиденциальности
Кви про кво	Ознакомление с политикой конфиденциальности

Таким образом, система защиты информации для объекта КИИ будет использовать как технические меры, так и организационные. К техническим относится использование программно-аппаратных средств: АВПО и МЭ. В качестве организационных мер выступают обучение пользователей ИС правилам использования ресурсов интернета и ознакомление с политикой конфиденциальности. Если ориентироваться на возможные затраты, то обучение и ознакомление должно носить тестовый характер внутри организации с занесением данных в «Журнал учета пользователей».

Итоговый алгоритм по разработке модели нарушителя и угроз безопасности информации объекта КИИ в упрощенном виде имеет следующий вид (рис. 3).

Рисунок 3 – Алгоритм по разработке модели нарушителя и угроз безопасности информации объекта КИИ

Заключение. В данной статье представлена теоретическая база, которая станет основой для разработки программного комплекса.

Данная теоретическая база включает в себя модель нарушителя и угроз для объектов КИИ. Рассмотрен процесс категорирования объектов критической информационной инфраструктуры, представлен алгоритм непосредственно расчета актуальности угроз.

Новым в данной теоретической базе является введение человеческого фактора и угроз, связанных с использованием методов социальной инженерии. Также разработка этой базы осуществлялась в условиях методической неопределенности, что повышает актуальность работы.

Библиографический список

1. Бердник М. В. Структура органов государственной власти в области безопасности критической информационной инфраструктуры / М. В. Бердник, М. Б. Гострый, Е. Ф. Новикова // Вопросы кибербезопасности,

моделирования и обработки информации в современных социотехнических системах. – 2018. –№ 6. – С. 85–92.

2. Глухов А. П. Моделирование процессов нарушения информационной безопасности критической инфраструктуры / А. П. Глухов, Горбачев И. Е. // Труды СПИИРАН. – 2015. – Вып. 38. – С. 112–135.

3. Новикова Е. Ф. Критическая информационная инфраструктура: модель безопасности / Е. Ф. Новикова, В. Н. Хализев // Социотехнические и гуманитарные аспекты информационной безопасности : материалы Всероссийской научно-практической конференции. – Пятигорск : ПГУ, 2019. С. 247–252.

4. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах». 2014 г. – 176 с. – Режим доступа: https://fstec.ru/component/attachments/download/675, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.09.2019).

5. Методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». – 2008. – 69 с. – Режим доступа: https://fstec.ru/component/attachments/download/289, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.09.2019).

6. Методический документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». – 2008. – 10 с. – Режим доступа: https://fstec.ru/component/attachments/download/290, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.09.2019).

7. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (проект). – 2015. – 43 с. – Режим доступа: http://fstec.ru/component/attachments/download/812, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.09.2019).

8. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_290595, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 16.09.2019).

9. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрировано в Минюсте России 26.03.2018 № 50524). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_294287, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 17.09.2019).

10. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 15.09.2019).

11. Чернигин Ю. Социальная инженерия. Вводный материал. – Режим доступа: https://www.volgablob.ru/blog/?p=1722, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.09.2019).

12. Methodologies for the identification of Critical Information Infrastructure assets and services. – Режим доступа: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 10.09.2019).

References

1. Berdnik M. V., Gostryy M. B., Novikova E. F. Struktura organov gosudarstvennoy vlasti v oblasti bezopasnosti kriticheskoy informatsionnoy infrastruktury [Structure of governmental departments in the field of providing the security of critical information infrastructure]. *Voprosy kiberbezopasnosti, modelirovaniya i obrabotki informatsii v sovremennykh sotsiotekhnicheskikh sistemakh* [Problems of Cybersecurity, Modeling and Information Processing in Modern Socio-technical Systems], 2018, issue 6, pp. 85–92.

2. Glukhov A. P., Gorbachev I. E. Modelirovanie protsessov narusheniya informatsionnoy bezopasnosti kriticheskoy infrastruktury [Modeling the processes of violation of information security of critical infrastructure]. *Trudy SPIIRAN* [Scientific works of SPIIRAS], 2015, issue 38, pp. 112–135.

3. Novikova E. F., Khalizev V. N. Kriticheskaya informatsionnaya infrastruktura: model bezopasnosti [Critical Information Infrastructure: Security Model]. *Sotsiotehnicheskie i gumanitarnye aspekty informatsionnoy bezopasnosti : materialy Vserossiyskoy nauchno-prakticheskoy konferentsii* [Sociotechnical and humanitarian aspects of information security : Materials of the All-Russian Scientific and Practical Conference]. Pyatigorsk, Pyatigorsk State University, 2019, pp. 247–252.

4. *Metodicheskiy dokument FSTEK Rossii "Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh"* [Guidance document of the FSTEC of Russia "Information security measures in state information systems"], 2014, 176 p. Available at: https://fstec.ru/component/attachments/download/675 (accessed 18.10.2019).

5. *Metodicheskiy dokument FSTEK Rossii "Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh"* [Guidance document of the FSTEC of Russia "The basic model of personal data security threats when they are processed in personal data information systems"], 2008. 69 p. Available at: https://fstec.ru/component/attachments/download/289 (accessed 15.09.2019).

6. *Metodicheskiy dokument FSTEK Rossii "Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh"* [Guidance document of the FSTEC of Russia "Methodology for determining current threats to the security of personal data during their processing in personal data information systems"], 2008. 10 p. Available at: https://fstec.ru/component/attachments/download/290 (accessed 15.09.2019).

7. *Metodicheskiy dokument FSTEK Rossii "Metodika opredeleniya ugroz bezopasnosti informatsii v informatsionnykh sistemakh" (proekt)* [Guidance document of the FSTEC of Russia "Methodology for identifying threats to information security in information systems" (project)], 2015. 43 p. Available at: http://fstec.ru/component/attachments/download/812 (accessed 18.09.2019).

8. *Postanovlenie Pravitelstva RF ot 08.02.2018 № 127 "Ob utverzhdenii Pravil kategorirovaniya obektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriev znachimosti obektov kriticheskoj informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy"* [Decree of the Government of the Russian Federation dated February 8, 2018 no. 127 "On Approval of the Rules for the Categorization of Objects of Critical Information Infrastructure of the Russian Federation, as well as a list of indicators of criteria of significance of objects of critical information infrastructure of the Russian Federation and their values"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_290595 (accessed 16.09.2019).

9. *Prikaz FSTEK Rossii ot 25.12.2017 № 239 "Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh obektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii"* [Order of the FSTEC of Russia dated December 25, 2017 no. 239 "On approving the Requirements to ensure the security of significant objects of the critical information infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_294287 (accessed 17.09.2019).

10. *Federalnyy zakon ot 26.07.2017 № 187-FZ "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii"* [Federal Law dated 26.07.2017 no. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885 (accessed 15.09.2019).

11. Chernidin Yu. *Sotsialnaya inzheneriya. Vvodnyy material* [Social Engineering. Introductory material]. Available at: https://www.volgablob.ru/blog/?p=1722 (accessed 10.09.2019).

12. *Methodologies for the identification of Critical Information Infrastructure assets and services*. Available at: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis (accessed 10.09.2019).

DOI 10.21672/2074-1707.2019.48.4.135-143
УДК 004.056

КЛАССИФИКАЦИЯ МЕССЕНДЖЕРОВ НА ОСНОВЕ АНАЛИЗА УРОВНЯ БЕЗОПАСНОСТИ ХРАНИМЫХ ДАННЫХ

Статья поступила в редакцию 13.11.2019, в окончательном варианте – 22.11.2019.

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: msanya@yandex.ru

В статье представлен анализ и классификация мессенджеров на основе анализа уровня безопасности хранимых данных. Произведен обзор современного состояния рынка мобильного приложения класса IM и введены критерии оценки безопасности систем мгновенного обмена сообщениями на основе фактической реализации заявленных алгоритмов и методов шифрования. Рассмотрены аспекты в области безопасности, защиты и хранения данных мессенджеров: данные пользователя на устройстве, журналы событий, ключи шифрования, критичная информация в базах данных, защищенность мессенджеров от атак с физическим доступом к устройству. Производится изучение механизма мессенджера Signal: организация хранения данных и реализация принципов защищенности для хранимых данных. На его примере рассмотрены схемы реализации и использования баз данных мобильного устройства. Выявлены недостатки использования подсистем шифрования и организации баз данных телефонных номеров, отметок регистрации пользователей, текстовых сообщений и медиафайлов, в связи с чем появляется возможность автоматизированного съема критичной информации. В результате сформулированы рекомендации по обеспечению безопасности мессенджеров для разработчиков и пользователей: шифровать вложения мессенджера, переместить все данные из доступного для пользователя пространства памяти в закрытое хранилище приложения, использовать запутывающие названия файлов, шифровать критичные данные в базах данных (сообщения, путь к вложениям, информация о контактах и пр.), использовать дополнительный слой для шифрования критичных данных при условии включенной надстройки, обеспечивающей обязательность ввода парольной фразы для открытия приложения на смартфоне, шифровать непосредственно сами базы данных.

Ключевые слова: анализ, кибербезопасность, форензика, мессенджер, протокол шифрования, защита информации, база данных