ИСПОЛЬЗОВАНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРЕДОСТАВЛЯЕМЫХ ЧЕРЕЗ ИНТЕРНЕТ САЙТ

Ничипорчук Максим Михайлович,
аспирант, Национальный исследовательский ядерный университет «МИФИ»
Nichiporchuk@list.ru
05.13.19

Аннотация: *В статье описаны подходы к применению двухфакторной аутентификации пользователей на интернет сайтах для защиты персональных данных от неправомерного доступа. Предложен метод защиты с использованием SMS-сообщений. Приведен пример реализации данного метода. Выполнен анализ повышения защищенности с применением предлагаемого метода.*

Ключевые слова: информационная безопасность, двухфакторная аутентификация, персональные данные.

TWO-FACTOR AUTHENTICATION AS AN ADDITIONAL SECURITY LAYER FOR ACCESS TO PERSONAL DATA THROUGH AN INTERNET SITE

Nichiporchuk Maksim Mihailovich
graduate student, National Nuclear Research University «MEPHI»

Abstract: *This article describes approaches to applying the two-factor authentication for Internet sites to protect personal data from a non-legitimate access. Proposed a method of protection with the use of SMS-messages. An example of this method. The analysis of more secure with the use of the proposed method.*

Keywords: Security, Two-factor authentication, personal data.

Согласно Федеральному Закону №152 «О персональных данных» [1] информационные системы, которые работают с персональными данными, должны быть защищены в соответствии с требованиями законодательства. Защите подлежит любая зафиксированная информация, неправомерное обращение с которой может нанести ущерб ее владельцу — физическому лицу. Организации системы здравоохранения, медицинские учреждения, фонды обязательного медицинского страхования, страховые медицинские компании являются операторами персональных данных. Их информационные системы обрабатывают не только демографическую, финансовую, но и медицинскую информацию. Также как и операторы персональных данных из других секторов, например, телекоммуникационного, финансового, они начали адаптировать свои информационные системы персональных данных (ИСПДн) к требованиям госрегуляторов, внедряя соответствующие решения.

Информационной системой, работающей с персональными данными, может быть интернет сайт медицинского учреждения, предоставляющий сервисы пациентам для доступа к их личной информации.

Согласно закону персональные данные определяются как любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [1].

Согласно базовой модели угроз, при обработке ПДн в локальных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационно-

го обмена, возможна реализация следующих угроз безопасности персональных данных:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте [2].

Предлагаемый в данной статье метод, направлен на снижение угроз НСД к ПДн, обрабатываемым на автоматизированном рабочем месте. Методы для снижения риска реализации угроз, связанные с утечкой информации по техническим каналам не рассматриваются.

Двухфакторная аутентификация – форма аутентификации, при которой используется комбинация двух факторов аутентификации. Как правило, различают три типа факторов: то что мы знаем (пароль, ПИН-код), то что мы имеем (мобильный телефон, смарт-карта) и кем мы являемся (отпечатки пальцев, сетчатка глаза и т.д.).

Пример реализации

Рассмотрим двухфакторную аутентификацию, при которой используется одновременно: пароль + устройство. Фактор «пароль» будет обеспечиваться стандартной парольной аутентификацией на сайте. Фактор «устройство» – мобильный телефон пациента.

Суть предлагаемого метода – расширение стандартной модели доступа посредством введения дополнительной метки для веб-сессии. При этом каждый раз при обращении к разделам сайта, содержащих персональные данные, происходит проверка на наличие метки в рамках текущей веб-сессии.

Общая схема прохождения дополнительной аутентификации представляет следующую последовательность шагов:

- Шаг 1. Успешная аутентификация на сайте с помощью пароля;
- Шаг 2. Отправка SMS-сообщения с ПИН-кодом пользователю на его мобильный телефон;
- Шаг 3. Отображение экрана ввода ПИН-кода при попытке перехода в раздел, содержащий персональные данные;
- Шаг 4. Если ПИН-код введен верно, сессия помечается как активная, разрешается доступ.

Отправка SMS-сообщений

На сегодняшний день имеется множество провайдеров, предоставляющих услуги отправки SMS-сообщений. В данной статье не рассматриваются методы отправки сообщений.

Генерация ПИН-кода

Для удобства пользователя ПИН-коды должны быть короткими и запоминающимися «с первого взгляда». На практике чаще всего используют длину кода от 4 до 6 символов. ПИН-коды могут быть как цифровыми, так и буквенно-цифровыми. Однако следует иметь ввиду то, что многие SMS-провайдеры по умолчанию блокируют отправку SMS-сообщения, содержащего цифровые последовательности. Для разрешения данной проблемы необходимо связываться с провайдером для подтверждения того, что вам отправка подобных сообщений необходима для достижения ваших бизнес целей.

Хранение информации

Т.к. информацию о доступе к разделам сайта, содержащих персональные данные, необходимо где-то хранить, то проще всего это делать с помощью тех же средств, что и использует веб сервер для хранения материалов сайтов и служебной информации.

Схема данных предполагает наличие таблицы с полями, указанными в таблице ниже.

Информация в данную таблицу вносится сразу после прохождения парольной аутентификации на сайте (см. шаг 1). Значение метки об активности – ЛОЖЬ.

При прохождении дополнительного этапа аутентификации делается пометка, что в рамках данной сессии пользователю разрешен доступ к определенному разделу данных, хранящему персональную информацию.

Поле	Тип	Описание
Идентификатор записи таблицы	Число	
ПИН-код	Текст	
Идентификатор веб-сессии	Текст	
Метка активности	Бит	содержит значение ИСТИНА, если в рамках данной сессии разрешен доступ к разделам сайта, содержащих персональные данные, т.е. в случае успешного прохождения дополнительной аутентификации

Анализ защищенности

При использовании двухфакторной аутентификации для получения доступа к защищаемым данным злоумышленнику нужно знать логин пользователя, пароль и иметь в своем распоряжении его устройство (например, мобильный телефон). Вероятность этого достаточно мала, если учесть, что нужно не только завладеть логином жертвы, но и выкрасть у нее устройство аутентификации.

Кроме того, пропажа устройства быстро обнаруживается пользователем, после чего он может принять соответствующие меры по блокированию своей персональной информации. В случае использования лишь парольной аутентификации пользователь может даже не подозревать о том, что его пароль был взломан.

Очевидно, что риск совершения неправомерного доступа к защищаемой информации прямо зависит от затрат злоумышленника на взлом.

Проанализируем затраты на взлом при использовании в ИС парольной аутентификации и двухфакторной аутентификации.

Пусть X – стоимость взлома пароля, Y – стоимость получения устройства, Z – стоимость получения или подбора PIN-кода. Рассчитаем суммарную стоимость для каждого метода аутентификации:

$$S_{парол} = X \quad (1)$$

$$S_{двухфак} = X + Y + Z \quad (2)$$

Видим, что суммарная стоимость при использовании двухфакторной аутентификации выше, и соответственно вероятность взлома уменьшается.

Все изложенные выше факторы свидетельствуют о повышении степени защищенности персональных данных на сайте при внедрении методов защиты, использующих многофакторную аутентификацию.

Оценка снижения рисков нарушения информационной безопасности с получением количественных оценок проводится на определенном защищаемом объекте с участием группы экспертов [3], использующей технологии (методики) управления информационными рисками (идентификация рисков, оценивание рисков, оценка субъективной вероятности, оценка ущерба, метод оценки угроз и уязвимостей CRAMM).

Заключение

Предлагаемый метод обеспечивает более надежную защиту сайта от неправомерного доступа к персональной информации пользователей. На примере показана простота реализации метода.

Показано повышение защищенности информации на сайте и снижение риска нарушения информационной безопасности при внедрении предлагаемого метода. Идеи, изложенные в данной статье, применимы к любым веб приложениям любых сфер деятельности.

Список литературы

1. Федеральный закон РФ от 27 июля 2006 года №152-ФЗ «О персональных данных».
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), ФСТЭК, 2008.
3. Варфоломеев А.А. Управление информационными рисками: Учеб. пособие. – М.: РУДН, 2008. – 158 с.: ил.