DOI https://doi.org/10.46845/2541-8254-2022-5(37)-11-11

УДК 004.056.5

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-СЕРВИСОВ

И.А. Шикота студент 4-го курса,
e-mail: ilya.shickota@yandex.ru
ФГБОУ ВО «Калининградский государственный университет»,

М.В. Соловей, к.э.н., научный руководитель
e-mail: marina.solovej@klgtu.ru
ФГБОУ ВО «Калининградский государственный университет»

В данной статье проанализированы методы обеспечения информационной безопасности пользователей сети Интернет. В работе представлено описание угроз информационной безопасности, возникающих по причине получения злоумышленниками персональных данных пользователей интернет-сервисов, а также приведены примеры утечек информации, также повлекшие за собой угрозу пользователям. Сформулирован и обоснован необходимый комплекс мер для обеспечения информационной безопасности пользователей.

Ключевые слова: *информационная безопасность, злоумышленник, личные данные, пароль, аутентификация, утечка.*

ВВЕДЕНИЕ

Современное общество в значительной степени зависит от информационного обеспечения. Каждый человек в той или иной мере пользуется услугами и сервисами, которые предоставляет Интернет. Однако наряду со значительными удобствами и перспективами, которые предоставляет всемирная сеть, возникают различные угрозы киберпреступности, а именно утечки и кражи персональных данных пользователей сети, использующих различные сервисы для решения своих проблем.

ОБЪЕКТ ИССЛЕДОВАНИЯ

Объектом данного исследования являются применяемые в интернет-сервисах методы обеспечения информационной безопасности пользователей.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Целью данного исследования является разработка предложений по обеспечению информационной безопасности пользователей интернет-сервисов.

Для выполнения цели был составлен следующий список задач:

- изучить угрозы, возникающие при несанкционированном получении личной информации третьими лицами;
- изучить причины возникновения утечек данных;
- изучить современные способы обеспечения информационной безопасности;
- оценить качество обеспечения информационной безопасности пользователей для современных российских сервисов;
- составить и обосновать необходимый комплекс мер для обеспечения информационной безопасности пользователей.

МЕТОДЫ ИССЛЕДОВАНИЯ

В работе были использованы следующие методы научного исследования: анализ, синтез, дедукция, наблюдение, сравнение, измерение.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Для получения многих услуг людям в настоящее время не обязательно лично приходить в физическое место их оказания, достаточно воспользоваться интернет-сервисами. Как правило, в зависимости от вида услуги может понадобиться регистрация, а в процессе регистрации придётся вводить личные данные. Это необходимо для оказания услуги, но является потенциально опасным действием. Дело в том, что к личным данным пользователей могут получить несанкционированный доступ третьи лица. Что они могут сделать с помощью личных данных? Перед злоумышленниками открывается значительный спектр возможностей, вот часть из них:

- продать ваши личные данные. Они могут понадобиться другим злоумышленникам;
- узнать больше о владельце личных данных, что может упростить доступ в другие его аккаунты;
- заняться интернет-мошенничеством, представляясь личностью жертвы;
- в некоторых случаях, если владельцем является высокопоставленный сотрудник предприятия, то с помощью его аккаунта можно заниматься саботажем.

Как злоумышленники могут получить доступ к личным данным? У них много способов кражи данных [1]. Приведем основные:

- социальная инженерия, то есть совокупность приёмов, когда злоумышленник получает доступ к конфиденциальной информации через людей, а не из-за слабой неуязвимости сервисов [2];
- уязвимости в системе. Их наличие является следствием недостаточно тщательного проектирования составляющих информационной безопасности сервисов. Если злоумышленник сможет воспользоваться уязвимостями, то сможет украсть личные данные пользователей данного сервиса;
- изучение информации в общем доступе. К примеру, если человек создаёт посты в социальных сетях, то, возможно, среди данных постов будет информация о потенциальном секретном вопросе. В свою очередь, секретный вопрос используется для восстановления доступа к аккаунту, а значит, может применяться злоумышленником для взлома;
- физическое воздействие. К данному способу относятся: кража запоминающих устройств, документов, ноутбуков и телефонов, т. е. всего, что может обеспечить доступ к информации;
- ошибки, вызванные человеческими факторами. К примеру, злоумышленник может воспользоваться ситуацией, когда сотрудник забыл установить пароль доступа к конфиденциальной информации, и присвоить его:
- использование специализированных инструментов для взлома по методу “грубой силы”.

Очевидно, что на протяжении длительного времени постоянно создаются новые способы по обеспечению информационной безопасности, где, в зависимости от способа кражи информации, будет отличаться способ противодействия.

Методы борьбы с воздействием социальной инженерии заключаются в повышении осведомлённости сотрудников о важности информации, которой они владеют, разъяснении принципов социальной инженерии, создании чётких инструкций. Также можно проводить разъяснительную работу с пользователями и формировать у них навыки, позволяющие

предотвратить утечки информации [3]. Разработаны представленные ниже простые правила, которые нужно объяснить всем людям:

- никому и никогда не сообщать свои логины и пароли, даже когда вас пытаются убедить в необходимости совершения таких действий;
- при обнаружении подозрительных ссылок в письме всегда уточнять у отправителя через другие каналы связи, что это письмо действительно от него и что эта ссылка не ведёт на вредоносный ресурс;
- блокировать компьютер, когда пользователь от него отходит;
- для каждого сервиса устанавливать уникальный и нетривиальный пароль.

В отличие от социальной инженерии, методы взлома через программные уязвимости сервисов уже не предполагают взаимодействие с владельцами информации напрямую. Потому обычные пользователи сервисов никак не могут повлиять на данные методы взлома. Максимум, что они могут сделать, при обнаружении различных ошибок или недочётов - сообщить об этом разработчикам сервиса через систему обратной связи или иным способом.

Предположим, что сотрудники организации проинформированы о важности информации, которой они владеют, максимально критично рассматривают все письма и обращения, и потому они неуязвимы для методов социальной инженерии. Также предположим, что в системе абсолютно нет уязвимостей. Будет ли в таком случае достигнута абсолютная защищённость? Конечно, нет. Пароль, как ни странно, можно просто подобрать с помощью специализированных средств. В таком случае время подбора будет зависеть от возможного алфавита и длины пароля. Ниже представлена таблица с продолжительностью взлома пароля. Предполагается, что в нем могут использоваться 36 символов, а скорость перебора паролей 100000 в секунду. В таблице 1 представлено время взлома паролей в зависимости от количества знаков [4].

Таблица 1 - Время взлома пароля в зависимости от количества знаков

Кол-во знаков	**Кол-во вариантов**	**Стойкость**	**Время перебора**
1	36	5 бит	Менее секунды
2	1296	10 бит	Менее секунды
3	46 656	15 бит	Менее секунды
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 часов
7	78 364 164 096	36 бит	9 дней
8	$2{,}821\ 109\ 9 \times 10^{12}$	41 бит	11 месяцев
9	$1{,}015\ 599\ 5 \times 10^{14}$	46 бит	32 года
10	$3{,}656\ 158\ 4 \times 10^{15}$	52 бита	1 162 года
11	$1{,}316\ 217\ 0 \times 10^{17}$	58 бит	41 823 года
12	$4{,}738\ 381\ 3 \times 10^{18}$	62 бита	1 505 615 лет

Из данных таблицы 1 следует, что для большинства ситуаций длины пароля в 10 символов достаточно.

При регистрации в сервисе в нём должна остаться запись о пароле для будущей аутентификации. Пароль может храниться в базе данных сервиса двумя способами: в неизменённом виде либо в виде хеша, сгенерированного алгоритмом хеширования в сервисе.

Теперь представим, что уязвимости есть, и утечка базы данных сервиса может произойти. Если пароли хранятся непосредственно в базе данных сервиса, то, когда случится утечка, у злоумышленников не будет никаких преград воспользоваться ими для

аутентификации. Получается, что в данной ситуации стойкость пароля не играет никакой роли.

Если же пароли хранились в базе данных в виде хеша, то всё зависит от алгоритма хеширования. К примеру ранее распространённый алгоритм шифрования MD5 подвержен взлому и потому в использовании фактически бесполезен. Алгоритм SHA-1 также был относительно недавно взломан, и потому от него отказались. В настоящее время популярными и не взломанными алгоритмами хеширования являются: семейство алгоритмов SHA-2, алгоритм SHA-3. Рациональнее всего будет использовать эти алгоритмы для хеширования.

Рассмотрим ситуацию, когда у злоумышленника есть и логин и пароль для доступа в сервис. В таком случае сохранность данных обеспечит только двухфакторная аутентификация. Это дополнение к привычной паре логина и пароля, связанное с вещью, которой владеет именно реальный владелец аккаунта. Такой вещью может быть смартфон с номером SIM карты, на который приходит SMS-код, либо специальное приложение, генерирующее коды в определённые промежутки времени параллельно с таким же генератором на стороне сервиса, либо специализированный usb-ключ и смарт-карты. Также благодаря двухфакторной аутентификации можно настроить уведомления о несанкционированных попытках доступа в аккаунт, что позволит принять необходимые меры по защите информации.

Пренебрежение методами защиты информации может дорого обойтись предприятиям. Ниже представлены примеры утечек данных, которые иллюстрируют серьезность обсуждаемой проблемы:

- утечка данных из сервиса “Яндекс еда” [5]. Были опубликованы ФИО пользователей, адреса доставки, комментарии к заказам. Далее были предприняты несколько коллективных исков к компании с требованием компенсации морального вреда [6] [7]. На момент написания статьи информации о начислении выплат пострадавшим не было. Необходимо отметить, что с такими данными, как ФИО, адрес проживания, комментарии к заказу, человек становится уязвимее для методов социальной инженерии. Следовательно, из-за данной утечки у злоумышленников стало больше возможностей получить доступ к другим сервисам;
- утечка данных из федеральной сети лабораторий “Гемотест” [8]. Компания свою вину отрицает. В результате данной утечки были получены: ФИО, дата рождения, адрес, телефон, номер паспорта [9]. Помимо вышесказанных угроз, из-за наличия в утечках паспортных данных злоумышленники могут оформлять кредиты, имущество, регистрировать предприятия и так далее.

В обоих случаях компании практически не понесли экономического ущерба, штрафы составили 100 тыс. руб. для сервиса “Яндекс еда” и 60 тыс. руб. для федеральной сети “Гемотест”, что совершенно незначительно в сравнении с угрозами, которыми теперь подвержены жертвы утечек. Штрафы в Российской Федерации слишком низкие для компаний.

Денежные взыскания за несохранность личных данных для компаний должны быть увеличены с целью повышения информационной безопасности пользователей. Либо компании самостоятельно повысят уровень защиты данных, либо будут платить штрафы, которые следует направлять на помощь пострадавшим от утечек и на повышение степени защищённости сервисов.

Несомненно, является положительным тот факт, что Министерство цифрового развития, связи и массовых коммуникаций (далее – Минцифры) готовит новую версию законопроекта об оборотных штрафах за утечку персональных данных: оборотные штрафы, на введении которых настаивает Минцифры, будут исчисляться в процентах от выручки компаний. Так, оборотный штраф в 1 % для компании с выручкой в 100 млрд руб. составит 1 млрд руб. [10].

ЗАКЛЮЧЕНИЕ

Резюмируя вышесказанное, можно выделить два направления по обеспечению информационной безопасности: для компаний, владеющих и управляющих интернет-сервисами и для физических лиц.

Предлагается использовать следующий комплекс мер, который необходим для предотвращения утечек информации, относящейся к пользователям интернет-сервисов:

- использовать для формирования хешей паролей пользователей алгоритм хеширования SHA-3 или семейство алгоритмов хеширования SHA-2. Допускается применение других алгоритмов хеширования, не взломанных на текущий момент. Но необходимо отметить, что рекомендуется использовать SHA-3, так как он опубликован в качестве стандарта FIPS 202 [11];
- оповестить своих сотрудников о методах социальной инженерии, используемых злоумышленниками, а также способам противодействовать утечкам информации в результате применения этих методов. В рамках этого следует создать и выдать специальные справочники для сотрудников, организовать горячие линии для быстрого их обращения по подозрениям в социальном хакерстве;
- уменьшить количество информации, которой владеют сотрудники, в зависимости от их обязанностей. Чем меньше сотрудник знает, тем меньше угроза от успешного воздействия злоумышленников методами социальной инженерии или собственных ошибок сотрудника;
- установить для пароля обязательное условие: не менее 10 символов при 36-значном алфавите. При данной длине подбор пароля методом “грубой силы” будет занимать значительное время, потому будет нецелесообразным;
- внедрить двухфакторную аутентификацию. Данный инструмент значительно усилит защиту информации благодаря тому, что коды доступа будут приходить на конкретное устройство сотрудника;
- обязать пользователей периодически менять пароли. Факт того, что пароль известен злоумышленникам, может остаться неизвестным до момента атаки. Значит, чтобы избегать таких ситуаций, необходимо периодически менять пароли.

СПИСОК ЛИТЕРАТУРЫ

1) “Что такое кража данных и как ее избежать” [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/resource-center/threats/data-theft (дата обращения 04.11.2022);

2) Социальная инженерия и социальные хакеры /М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2007. — 368 с.: ил. Аннотация (дата обращения 04.11.2022);

3) “Социальная инженерия: актуальная угроза и меры защиты” [Электронный ресурс]. Режим доступа: https://safe-surf.ru/users-of/article/642870/ (дата обращения 04.11.2022);

4) “Пример продолжительности подбора паролей” [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Полный_перебор (дата обращения 04.11.2022);

5) “Служба безопасности Яндекс Еды сообщила об утечке информации” [Электронный ресурс]. Режим доступа: https://yandex.ru/company/services_news/2022/01-03-2022 HYPERLINK "https://yandex.ru/company/services_news/2022/01-03-2022"(дата обращения 04.11.2022);

6) “Клиенты подали коллективный иск к «Яндекс.Еде» за утечку данных” [Электронный ресурс]. Режим доступа: https://www.sravni.ru/novost/2022/3/30/klienty-podali-kollektivnyj-isk-k-yandeks-ede-za-utechku-dannyh/ (дата обращения 04.11.2022);

7) “Клиенты «Яндекс.Еды» подали ещё один коллективный иск за утечку данных” [Электронный ресурс]. Режим доступа: https://www.sravni.ru/novost/2022/4/14/klienty-yandeks-edy-podali-eshhyo-odin-kollektivnyj-isk-za-utechku-dannyh/ (дата обращения 04.11.2022);

8) “«Гемотест» оштрафовали на 60 тыс. руб. за утечку персональных данных ” [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5480244 (дата обращения 04.11.2022);

9) “В даркнете выставили на продажу данные клиентов «Гемотеста»” [Электронный ресурс]. Режим доступа: https://www.sravni.ru/novost/2022/5/4/v-darknete-vystavili-na-prodazhu-dannye-klientov-gemotesta/ (дата обращения 04.11.2022);

10) “Минцифры готовит новую версию законопроекта об оборотных штрафах за утечку персональных данных ” [Электронный ресурс]. Режим доступа: https://digital.gov.ru/ru/events/41722/ (дата обращения 04.11.2022);

11) FIPS202 [Электронный ресурс]. Режим доступа: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (дата обращения 04.11.2022);

DEVELOPMENT OF A SET OF MEASURES TO ENSURE THE INFORMATION SECURITY OF USERS OF INTERNET SERVICES

I.A. Shikota, 4nd year student
e-mail: ilya.shickota@yandex.ru
Kaliningrad State Technical University

M.V. Solovej, PhD, Associate professor
e-mail: marina.solovej@klgtu.ru
Kaliningrad State Technical University

The article analyzes the methods for ensuring information security of the Internet users. The paper presents a description of information security threats arising from the receipt by attackers of personal data of users of Internet services, as well as examples of information leaks that also led to a threat to users. The necessary set of measures to ensure the information security of users has been formulated and justified.

Key words: *information security, intruder, personal data, password, authentication, leak.*