Красников В. В.

ОСНОВЫ БЕЗОПАСНОСТИ ДАННЫХ В ИНТЕРНЕТЕ

В 2016 году мир целиком захвачен огромным количеством различных социальных сетей и сервисов, предоставляющих пользователям собственные хранилища. Люди ежедневно загружают в интернет гигабайты информации о себе: видео из своей жизни, фотографии и текстовые данные о своем месторасположении, о своих вкусах, предпочтениях и действиях. Удаление же контента в том случае, если пользователь пожалеет о написанном сообщении или залитом фото, не поможет, так как данные все равно сохранятся где-то там, на серверах корпорации Twitter inc. или facebook.

Есть масса примеров «громких» ситуаций, связанных с недобросовестным хранением данных. Например, случай, связанный с корпорацией Apple, когда произошла утечка огромного количества личных фото звезд и знаменитостей. Или же публичное заявление исполнительного директора корпорации Apple о том, что ФБР попросили у Apple встроить бэкдор в операционную систему iOS для раскрытия какого-то одного дела. При этом некоторые считают, что это вообще целиком пиар ход со стороны Тима Кука, а в iOS уже давно есть подобные лазейки.

Фактически, даже находясь на локальном компьютере, данные не остаются в полной безопасности. Вирусы и трояны, которые попадают неопытным пользователям на их персональные компьютеры, уносят с собой хранимые пароли и прочий контент. Важным вопросом остается подход к созданию паролей для личных аккаунтов. При этом лучшим вариантом будет генерация случайной последовательности букв разного регистра и цифр. Отсутствие какой-либо логики при внушительной длине – это миллиарды комбинаций, подобрать нужную в данном случае будет практически невозможно даже при помощи «алгоритма» bruteforce.

Следует помнить, что данные, опубликованные в Интернете фактически невозможно стереть, а корпорации, предоставляющие хранилища для них, не могут обеспечить их полную сохранность и безопасность.