П. О. АБРАМОВ
(г. Гомель, Белорусский торгово-экономический
университет потребительской кооперации)
Науч. рук. **Н. В. Яцевич**,
канд. экон. наук, доц.

КРИПТОГРАФИЯ КАК МЕТОД ЗАЩИТЫ И СОКРЫТИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

На протяжении многих лет IT-технологии стремительно проникают во все сферы жизни современных людей, и со временем их влияние на нее становится все больше и больше, начиная от высокотехнологических, промышленных масштабов, до банальных «постов» в различных социальных сетях, таких как «Instagram», «Vkontakte». И на данный момент нет ни одной сферы, в которой хоть как-нибудь не были бы задействованы IT-технологии.

Современное промышленное предприятие не может существовать без информационных технологий, для того, чтобы выдерживать конкуренцию в условиях повсеместного использования высокотехнологичных решений. Однако, логично предположить, что с ростом информатизации увеличивается риск утечки информации в следствие слабой криптографии, ведь в наше время ИТ-технологии многие используют для перехвата информации, что абсолютно недопустимо для современных конкурентноспособных организаций.

Криптография (или криптология; от греческого kryptós, «скрытый, секретный»; и graphein, «письмо») - это практика и изучение методов для безопасного общения в присутствии третьих лиц (называемых противниками) [1]. В более общем плане речь идет о построении и анализе протоколов, блокирующих противников;

Основные функции криптографии:

– помогает обеспечить подотчетность, справедливость, точность и конфиденциальность;

– предотвращает мошенничество в электронной торговле и гарантировать действительность финансовых операций;

– защищает вашу анонимность и, в случае чего, может доказать вашу личность;

– может помешать вандалам изменять вашу электронную информацию и препятствовать промышленным конкурентам читать ваши конфиденциальные документы [2].

В настоящее время миллиарды долларов тратятся на компьютерную безопасность, и большая их часть тратится на небезопасные продукты. Ошибиться в данной ситуации очень просто, поскольку слабая криптография выглядит так же, как и сильная криптография. Например, два продукта шифрования электронной почты могут иметь почти одинаковый пользовательский интерфейс, но один из них безопасен, а другой может быть подвергнут риску взлома. Две программы могут иметь схожие функции, хотя одна из них имеет зияющие дыры в безопасности, которых нет у другой, и только опытный криптограф может выявить разницу.

Люди, которые взламывают криптографические системы, не следуют правилам, они являются мошенниками. Они могут атаковать систему, используя методы, о которых дизайнеры и разработчики используемого программного обеспечения никогда не думали. Криптографическая защита должна защищать от всех возможных уязвимостей, но злоумышленник может найти хотя бы один недостаток безопасности, чтобы поставить под угрозу всю систему.

Никто не может гарантировать 100 % безопасность. Но мы можем работать над принятием 100 % риска. Мошенничество существует в современных торговых систе- мах: наличные деньги могут быть подделаны, чеки изменены, номера кредитных карт украдены. Тем не менее, эти системы все еще успешны, потому что преимущества и удобства перевешивают потери. Системы конфиденциальности: стенные сейфы, двер- ные замки, шторы - не идеальны, но они часто достаточно хороши. Хорошая крипто- графическая система устанавливает баланс между тем, что возможно, и тем, что приемлемо.

Разработка криптографической системы – это тоже искусство. Дизайнер должен соблюдать баланс между безопасностью и доступностью, анонимностью и подотчетно- стью, конфиденциальностью и пригодностью. Наука сама по себе не может гарантиро- вать безопасность. В этом помогают опыт и интуиция. Криптография может помочь в проектировании новых систем безопасности и поиске дефектов в существующих.

Сильная криптография может противостоять целевым атакам вплоть до момента, когда становится легче получить информацию каким-то другим способом. Компьютер- ная программа шифрования, независимо от того, насколько она хороша, не помешает злоумышленнику пройти через чей-то «мусор». Но это может полностью предотвра- тить атаки по сбору данных, так как ни один злоумышленник не может пройти через огромное количество «мусора», чтобы найти информацию каждого в стране.

Современная компьютерная безопасность - это карточный домик; он может защи- щать сейчас, но он не может защищать вечно, требует постоянного совершенствования системы в соответствии с повышением риска утечки информации. Этот процесс носит непрерывный характер и заключается в реализации современных методов и способов совершенствования систем информационной безопасности, непрерывного мониторин- га, выявления ее слабых мест и потенциальных каналов утечки информации. Постоян- ное совершенствование систем связано с появлением новых способов доступа к ин- формации извне.

Список использованной литертуры

1 Криптография - Cryptography [Электронный ресурс]. – 2020. – Режим доступа: https://ru.qwe.wiki/wiki/Cryptography. – Дата доступа: 08.02.2020.

2 Защита информации. Криптография [Электронный ресурс]. – 2020. – Режим доступа: https://mirznanii.com/a/43338-5/zashchita-informatsii-kriptografiya-5. – Дата доступа: 09.02.2020.