К ВОПРОСУ О ЗАЩИТЕ ПОТОКОВ ДАННЫХ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стахно Р.Е.[1], Гончар А.А.[2], Васютина Т.Л.[3] Email: Stahno1135@scientifictext.ru

[1]Стахно Роман Евгеньевич - кандидат технических наук;
[2]Гончар Артем Александрович - кандидат военных наук;
[3]Васютина Татьяна Львовна – кандидат технических наук, доцент,
кафедра математики и информатики,
Санкт-Петербургский университет МВД России,
г. Санкт-Петербург

Аннотация: *несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается. В связи с этим понятие «защита информации» становится ключевым и рассматривается как процесс или деятельность, направленная на предотвращение утечки защищаемой информации, а также различного рода несанкционированных воздействий на информацию и ее носители. В статье анализируются проблемы, связанные с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи. Рассмотрены основные средства обеспечения защиты информации. Предложен алгоритм, используемый при создании зашифрованных данных.*
Ключевые слова: *защита информации, контаминированные средств, криптография, гаммирование.*

TO THE QUESTION OF PROTECTION OF DATA FLOWS AND ENSURING INFORMATION SECURITY

Stahno R.E.[1], Gonchar A.A.[2], Vasyutina T.L.[3]

[1]Stahno Roman Evgenyevich – PhD in Technical;
[2]Gonchar Artem Aleksandrovich – PhD in Military;
[3]Vasyutina Tatiana Lvovna - PhD in Technical, Assistant Professor,
DEPARTMENT OF MATHEMATICS AND INFORMATICS,
SAINT PETERSBURG UNIVERSITY OF MINISTRY OF INTERNAL AFFAIRS OF RUSSIAN FEDERATION,
ST. PETERSBURG

Abstract: *despite the increasing efforts to create data protection technologies, their vulnerability not only does not decrease, but also increases steadily. Therefore, the relevance of problems related to the protection of data flows and ensuring the information security of their processing and transmission is increasingly reinforced. As a result, the concept of "information protection" becomes key and is viewed as a process or activity aimed at preventing the leakage of protected information, as well as various Kind of unauthorized impacts on information and its carriers. The article analyzes the problems related to the protection of data flows and ensuring the information security of their processing and transmission. The basic means of securing information protection are considered. An algorithm used to create encrypted data is proposed.*
Keywords: *information protection, contaminated means, cryptography, gamming.*

УДК 004.056

С развитием новых информационных технологий и возрастающими усилиями по созданию более совершенных способов защиты данных, их уязвимость не уменьшается, а продолжает расти. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается. В связи с этим понятие «защита информации» становится ключевым и рассматривается как процесс или деятельность, направленная на предотвращение утечки защищаемой информации, а также различного рода несанкционированных воздействий на информацию и ее носители

Проблемы с защитой информации, как и источники угроз, по своей сущности различные, поэтому возникает необходимость в создании дифференцированных видов ее обеспечения.

Классифицировать средства обеспечения защиты информации можно на несколько групп:

1. аппаратные (технические) средства;
2. программные средства;
3. комбинированные средства;
4. организационные или административные средства.

К аппаратным (техническим) средствам относятся разные устройства. Они могут быть электронными, механическими или электромеханическими, но специфика их работы предполагает защиту информации посредством аппаратных средств. Применение этих устройств позволяет воспрепятствовать физическому проникновению или замаскировать данные, если доступ все же был открыт. Технические средства надежны, независимы от субъективных факторов и обладают высокой устойчивостью к модификации. Но и они обладают рядом недостатков, таких как высокая цена, они недостаточно гибкие и практически всегда обладают большими массой и объемом [1].

Программные средства позволяют контролировать доступ, проводить идентификацию пользователей, тестировать контроль системы защиты информации. Кроме того, средства, относящиеся к этой группе, могут шифровать данные и удалять рабочую (остаточную) информацию (вроде временных файлов).

Для обеспечения необходимой секретности информации применяют математические методы обеспечения конфиденциальности – криптографию или шифрование информации. При создании зашифрованных данных используют определенный алгоритм или устройство, которое его реализует. Изменяющийся код ключа осуществляет управление шифрованием. Именно с его помощью можно извлечь информацию.

Среди классических алгоритмов, которые используются, выделяют несколько основных:

1. Подстановка. Она может быть, как самой простой, одноалфавитной, так и многоалфавитной сложной (однопетлевой и многопетлевой).

2. Перестановка. Различают простую и усложненную.

3. Гаммирование. Речь идет о смешивании, в котором могут использовать длинную, короткую, неограниченную маски.

В первом случае исходный алфавит заменяется альтернативными. Это самый легкий способ шифрования. Данные, зашифрованные алгоритмом перестановки, будут более защищенными, ведь в нем используются цифровые ключи или эквивалентные слова.

Система, отдавшая предпочтение гаммированию, получит гарантию надежности и безопасности информации, потому что для осуществления этого способа шифрования будет проведена серьезная криптографическая работа. Для защиты используются нелинейные преобразования данных, методы рассечения-разнесения, компьютерная стеганография и прочее.

Контаминированные средства сочетают в себе свойства аппаратных (технических) и программных средств [2, 3].

К организационным или административным средствам относят средства защиты информации организационно-технического и организационно-правового характера. К ним относят:

- контроль доступа в помещения, их подготовку и оснащение;
- разработку стратегий безопасности организации;
- подборку и изучение национальных законодательств с последующим их применением;
- учреждение правил работы и контроль их соблюдения.

Полноценная защита информации может быть достигнута при использовании всех этих средств в комплексе.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Список литературы / References

1. *Домбровская Л.А., Яковлева Н.А., Стахно Р.Е.* Современные подходы к защите информации, методы, средства и инструменты защиты // Наука, техника и образование, 2016. № 4. С. 16-19.
2. *Стахно Р.Е., Гончар А.А.* Защита информации в современном документообороте // Наука, техника и образование, 2016. № 4. С. 19-21.
3. *Домбровская Л.А., Яковлева Н.А., Васютина Т.Л.* Организация защиты информации в персональных компьютерах // Наука и образование сегодня, 2016. № 9. С. 14-19.