Т. 8. №4. 2022
https://doi.org/10.33619/2414-2948/77

УДК 004.942 https://doi.org/10.33619/2414-2948/77/47

СОВРЕМЕННЫЕ СПОСОБЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

***©Абдыраева Н. Р.**, канд. техн. наук, Ошский технологический университет имени академика М. М. Адышева, г. Ош, Кыргызстан, nabdyraeva80@mail.ru*
***©Турсунбаев Ф. С.**, Ошский технологический университет имени академика М. М. Адышева, г. Ош, Кыргызстан, Gentle2907@gmail.com*
***©Жумабай уулу Н.**, Ош государственный университет, г. Ош, Кыргызстан, nurik_kg-93@mail.ru*

MODERN METHODS AND MEANS OF PROTECTING INFORMATION

***©Abdyraeva N.**, Ph.D., Osh Technological University named after academician M.M. Adyshev, Osh, Kyrgyz Republic, nabdyraeva80@mail.ru*
***©Tursunbaev F.**, Osh Technological University named after academician M.M. Adyshev, Osh, Kyrgyz Republic, Gentle2907@gmail.com*
***©Zhumabay uulu N.**, Osh State University, Osh, Kyrgyz Republic, nurik_kg-93@mail.ru*

Аннотация. Информационная безопасность - это процесс защиты данных от несанкционированного доступа, использования, раскрытия, уничтожения, изменения или нарушения. Информационная безопасность обеспокоена с конфиденциальностью, целостностью и доступностью данных независимо от формы, которую они могут принимать: электронные, печатные или другие формы. Эта статья представляет собой современные методы и способы защиты информации и законы и правила, регулирующие информационную безопасность.

Abstract. Information security is the process of protecting data from unauthorized access, use, disclosure, destruction, alteration or violation. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form it may take: electronic, print, or other forms. This article presents modern methods and techniques for protecting information and laws and regulations governing information security.

Ключевые слова: информационная безопасность, шифрование, дешифрование, метод перестановки, криптографические методы.

Keywords: Information security, encryption, decryption, reshuffle method, cryptographic methods.

Введение. Постановка задачи

Сегодня цифровые данные являются ключевым элементом большинства бизнес-процессов. Сбор, обработка и анализ больших объемов информации становится решающим конкурентным преимуществом компаний и государств. Информационная безопасность напрямую связана с ценностью информации. Риски возрастают, когда стоимость актива увеличивается. Где-то ценность выражается непосредственно в деньгах (интернет-банкинг, данные платежных карт, электронные кошельки), где-то сама конфиденциальная информация представляет собой важный цифровой актив (контракты, информация ДСП, базы данных клиентов и поставщиков, массивы персональных данных и т.д.).

Т. 8. №4. 2022
https://doi.org/10.33619/2414-2948/77

Вся информация, так или иначе, является ценным активом, и ее владелец несет риски при создании, сборе, использовании и хранении информации. Все проблемы информационной безопасности связаны с тем, что владельцы этих активов недооценивают свои риски и не принимают необходимых мер для обеспечения целостности, конфиденциальности и доступности данных.

До 2001 г законы Киргизской Республики не предусматривали определение понятия безопасности, а с принятием концепции национальной безопасности Киргизской Республики появилось нормативное определение этого понятия. 21 декабря 2021 г Указом Президента Кыргызстана утверждена действующая концепция национальной безопасности Кыргызстана, которая также включает вопросы информационной безопасности.

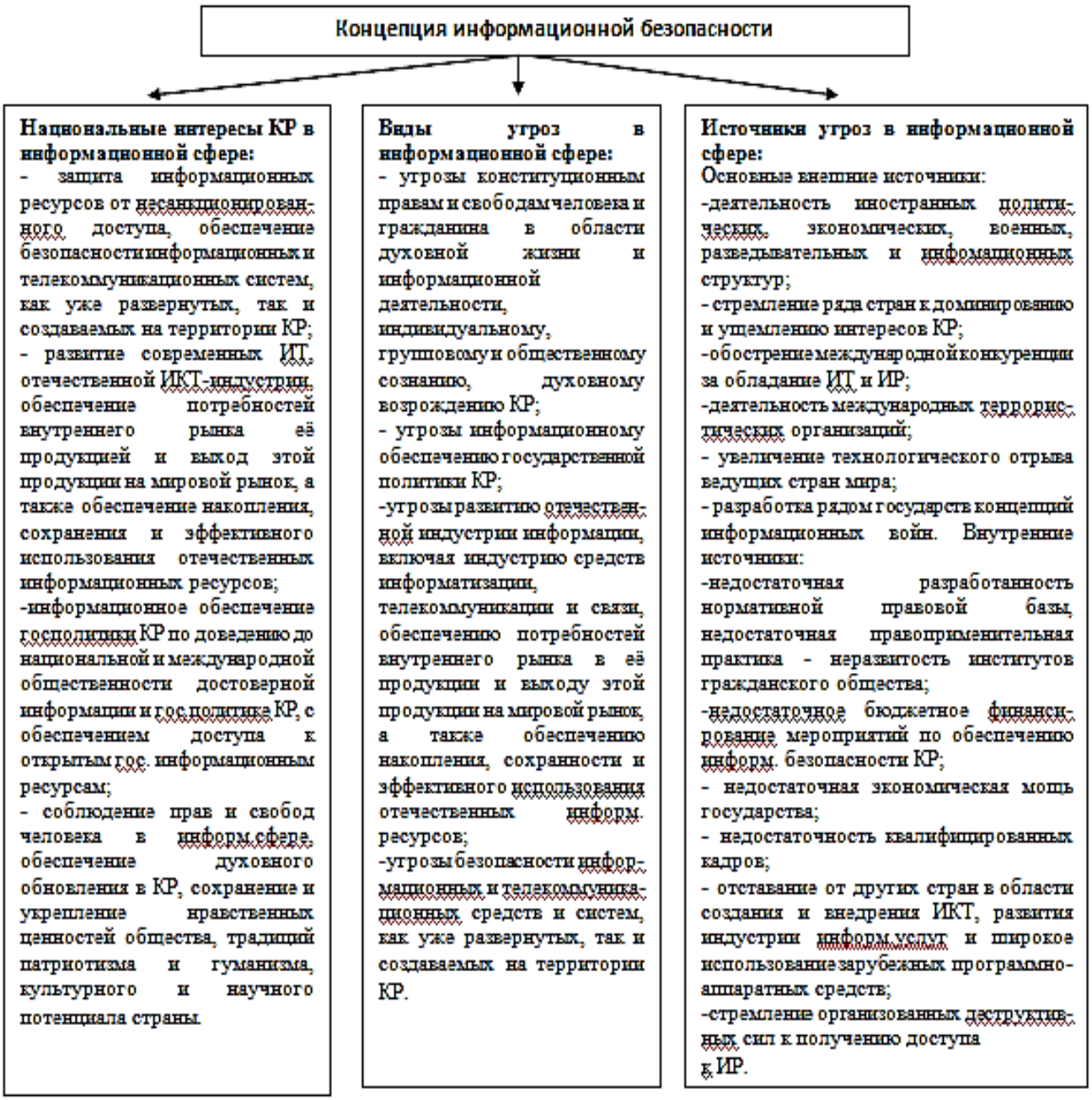

Рисунок 1. Концепция информационной безопасности

Т. 8. №4. 2022
https://doi.org/10.33619/2414-2948/77

В концепции (Рисунок 1) одна из внутренних угроз национальной безопасности страны определяется неразвитостью информационных и коммуникационных технологий и слабой защитой национального информационного пространства. Растущее использование Интернета делает борьбу с киберпреступностью и защиту информационной инфраструктуры, которая требует обширных мер в области сетей связи и информационной безопасности, особенно актуальной. Отсутствуют финансовые ресурсы для мер по защите информационного мира. Уголовный кодекс Кыргызстана устанавливает ответственность за преступления, связанные с информационными технологиями. К таким относится: создавать компьютерную программу или изменять существующую программу с намерением уничтожить, перехватить, изменить или скопировать информацию; прервать работу любого компьютера, компьютерной системы или ее сети; использовать или распространять любую такую программу или носителей таких программ.

Способы неправомерного доступа к информации

Ключом к успешному предотвращению несанкционированного доступа к информации и перехвату данных является четкое понимание пути утечки информации. Интегральные схемы, питающие компьютеры, производят высокочастотные изменения уровней напряжения и тока. Колебания распространяются по проводам и могут быть преобразованы в понятные формы и заблокированы специальными устройствами. Устройство может быть установлено на компьютер или монитор и перехватывать информацию, отображаемую на мониторе или вводимую с клавиатуры. Прослушивание возможно и при передаче информации по внешним каналам связи, например по телефонным линиям (https://clck.ru/SWDbp).

Методы защиты

На практике используется несколько групп способов защиты:

- воспрепятствование предполагаемому похитителю физическими и программными средствами;
- управлять или влиять на элементы защищаемой системы;
- маскирование или преобразование данных, обычно - криптографическим способом;
- разработка набора правил и мер для поощрения надлежащего поведения пользователей, взаимодействующих с правилами или базами данных.
- обеспечение соблюдения или создание таких условий, при которых пользователи обязаны соблюдать правила обработки данных;
- создание условий, которые побуждают пользователей действовать надлежащим образом.

Каждый метод защиты данных реализуется с использованием разных категорий средств. Основными средствами являются организационные и технические средства защиты информации.

Организационные средства защиты информации

За разработку комплекса средств организационной защиты информации должна отвечать служба безопасности.

В основном специалисты по безопасности:

- разработка внутренней документации, устанавливающей правила работы с компьютерной техникой и конфиденциальной информацией;
- проводить брифинги для персонала и периодические проверки;
- организовать подписание дополнений к трудовым договорам, регулирующих ответственность за разглашение или неправомерное использование информации, полученной в ходе работы;

Т. 8. №4. 2022
https://doi.org/10.33619/2414-2948/77

- разграничить зоны ответственности, чтобы исключить ситуации, когда у сотрудника самые важные данные;

- организуйте работу в популярных программах рабочего процесса и следите за тем, чтобы важные файлы не хранились на сетевых дисках;

- внедрять программные продукты, защищающие данные от копирования или уничтожения пользователями;

- составьте планы восстановления системы в случае сбоя по любой причине.

Если в компании нет собственной службы информационной безопасности, выход – пригласить специалиста по безопасности на аутсорс. Удаленный работник может проверить ИТ-инфраструктуру организации и дать рекомендации по защите от внешних и внутренних угроз. Аутсорсинг в сфере информационной безопасности также предполагает использование специальных программ для защиты корпоративной информации (https://clck.ru/exzDX).

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.

Чаще всего специалисты по безопасности:

-разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;

-проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;

-разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;

-внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;

-составляют планы восстановления системы на случай выхода из строя по любым причинам.

Если в компании нет выделенной ИБ-службы, выходом станет приглашение специалиста по безопасности на аутсорсинг. Удаленный сотрудник сможет провести аудит ИТ-инфраструктуры компании и дать рекомендации по ее защите от внешних и внутренних угроз. Также аутсорсинг в ИБ предполагает использование специальных программ для защиты корпоративной информации (https://clck.ru/exzDE).

Технические средства защиты информации

Группа технических средств защиты информации объединяет аппаратные и программные средства. В основном:

- резервное копирование и удаленное хранение наиболее важных областей данных в компьютерной системе;

- дублирование и резервирование всех важных для безопасности данных сетевых подсистем;

- создание возможности перераспределения сетевых ресурсов в случае выхода из строя отдельных элементов;

- обеспечение возможности использования систем аварийного электроснабжения;

- обеспечение сохранности оборудования от повреждений, вызванных пожаром или водой;

Т. 8. №4. 2022
https://doi.org/10.33619/2414-2948/77

- установка программного обеспечения, защищающего базы данных и другую информацию от несанкционированного доступа.

К техническим мерам относятся также мероприятия по обеспечению физической недоступности объектов компьютерной сети, например, такие практические методы, как оснащение помещений камерами и сигнализацией.

Аутентификация и идентификация

Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация. Идентификация — это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией. Аутентификация — это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск [1].

Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты — пароль. Многие люди в качестве пароля используют имена детей, родственников или год и дату рождения. Такая защита не является надежной. Кроме этого есть методы шифрования данных с помощью криптографических или методами перестановки. Процесс шифрования использует в качестве входных параметров объект — открытый текст и объект — ключ, а результат преобразования — объект — зашифрованный текст. При дешифровании выполняется обратный процесс. Далее рассмотрим программу для защиты данных методом перестановки (Рисунок 2).

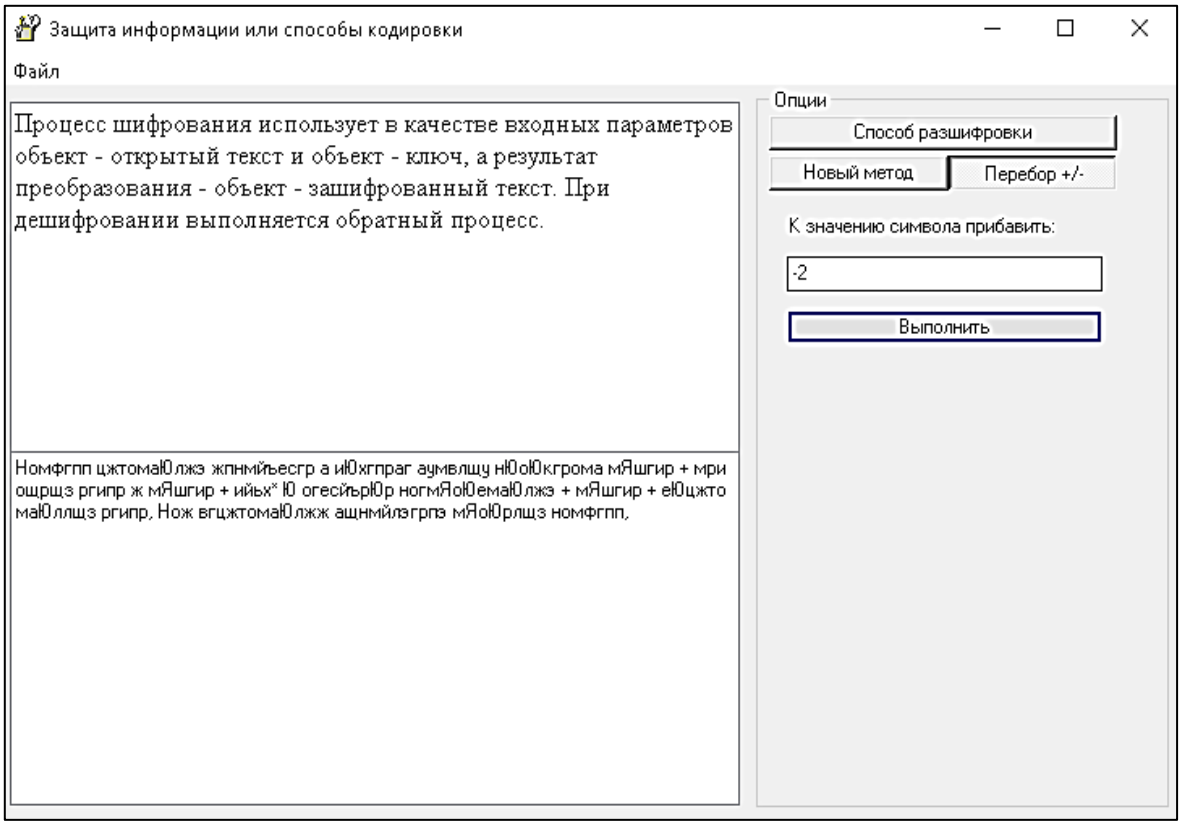

Рисунок 2. Работа программы

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить следующими формулами:

$$y = (x + k) \mod n$$
$$x = (y - k) \mod n,$$

где, {\displaystyle x}x — символ открытого текста, {\displaystyle y}y — символ шифрованного текста, {\displaystyle n}n — мощность алфавита, а {\displaystyle k}k — ключ. С точки зрения математики шифр Цезаря является частным случаемаффинного шифра.

Выводы:

Таким образом, в данной статье мы рассматривали концепцию информационной безопсности и современные методы и средства защиты информации. А также мы предлагаем защитить данные с помощью математических формул т.е. криптографическими методами.

Список литературы:

1. Ясенев В. Н. Информационная безопасность: Нижний Новгород, 2017. 198 с.

References:

1. Yasenev, V. N. (2017). Informatsionnaya bezopasnost': Nizhnii Novgorod. (in Russian).

Работа поступила
в редакцию 04.03.2022 г.

Принята к публикации
09.03.2022 г.

Ссылка для цитирования:

Абдыраева Н. Р., Турсунбаев Ф. С., Жумабай уулу Н. Современные способы и средства защиты информации // Бюллетень науки и практики. 2022. Т. 8. №4. С. 426-431. https://doi.org/10.33619/2414-2948/77/47

Cite as (APA):

Abdyraeva, N., Tursunbaev, F., & Zhumabay uulu, N. (2022). Modern Methods and Means of Protecting Information. *Bulletin of Science and Practice, 8*(4), 426-431. (in Russian). https://doi.org/10.33619/2414-2948/77/47