могают стандартизировать процессы защиты информации и минимизировать риски.

Нормативно-правовое регулирование и международные стандарты способствуют созданию безопасной среды для работы с информацией, задавая рамки и стимулируя компании к внедрению надёжных систем защиты. Нужно отметить, что безопасность – это не статичный процесс, а постоянная работа, включающая мониторинг и адаптацию к новым вызовам.

Таким образом, кибербезопасность и информационная безопасность – это не просто задача специалистов по защите, а ответственность на всех уровнях, от частных пользователей до государственных органов. Только при слаженной работе всех участников можно противостоять современным киберугрозам и обеспечить надёжную защиту данных в цифровом пространстве.

Литература

1. Обеспечение кибербезопасности в современных [Электронный ре-сурс]. – Режим доступа: https://rep.bntu.by/bitstream/handle/data/130299/260-264.pdf?sequence=1&isAllowed=y. – Дата доступа: 24.10.2024

2. Что такое кибербезопасность? [Электронный ресурс]. – Режим до-ступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security – Дата доступа: 25.10.2024

3. Киберугрозы и атаки: виды и методы защиты [Электронный ре-сурс]. – Режим доступа: https://sky.pro/wiki/profession/kiberugrozy-i-ataki-vidy-i-metody-zashity/ – Дата доступа: 26.10.2024

4. Что такое облачная безопасность? [Электронный ресурс]. – Режим доступа:https://www.oracle.com/cis/security/cloud-security/what-is-cloud-security/– Дата доступа: 30.10.2024

КРИПТОГРАФИЯ КАК НАУКА. ТИПЫ КРИПТОСИСТЕМ

Синяк У.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Повседневная жизнь человека неразрывно связана с информацией, с процессами её обработки, хранения и дальнейшей передачи. А вопросы информационной безопасности и сокрытия информации остаются одними из наиболее горячей темой в быстроразвивающемся мире.

Криптография, что в переводе с греческого означает «тайное письмо», появилась ещё с момента возникновения первой письменности на земле. С необходимостью передавать информацию возникла и необходимость скрывать её от лишних глаз. Люди хотели, чтобы информация могла передаваться привычным и

несложным для них путём, но при этом, содержание мог расшифровать лишь адресат. Это и послужило толчком к раннему развитию данной науки. [1]

С развитием электронных коммуникаций криптография становится всё более интересным предметом для широкого круга пользователей. К настоящему моменту повысилась необходимость защиты различного рода данных: не только коммерческих, но и персональных.

Сегодня под криптографией понимается наука о математических способах и методах обеспечения невозможности посторонним лицом прочесть передаваемую информацию и изменить её.

Простую модель криптографической системы можно описать следующим образом: существует информационная система, состоящая из отправителя (абонента А), получателя (абонента В) и канала, через который они будут общаться или, иными словами, передавать информацию через сообщения. В этой системе также существует вероятность возникновения незаконного пользователя (противника), который сможет перехватывать информацию, двигающуюся по каналу между абонентами. Стоит подчеркнуть, что противник может быть внутренним или внешним. Понятие «внутренний» предполагает, что противник входит в абоненты системы.

Вышеописанная модель может применяться не только в случаях передачи сообщений, но и в случаях защиты информации. Пользователь может одновременно являться абонентом А и абонентом В. Это происходит в случае работы с данными на компьютере в разное время. В этом случае «каналом» будет являться жёсткий диск компьютера.

Рассматривая модель, к каналу которой имеет доступ «противник», стоит отметить, что перед отправкой сообщения, отправитель преобразовывает его в шифртекст, то есть в закрытый текст. Такое преобразование называют *шифрованием*. Зашифрованный текст поступает к получателю, который расшифровывает его, то есть приводит к начальному виду.

Процедуры шифрования и расшифрования используют определённый инструмент, так называемый *ключ*. Ключ шифрования и ключ расшифрования могут совпадать – симметричные системы , и не совпадать – асимметричные системы .

Симметричные криптографические системы предполагают использование одного и того же инструмента – ключа для обращения зашифрованного сообщения в расшифрованное. В таких системах ключ является секретным. Симметричное шифрование предполагает, что ключ известен как отправителю, так и получателю. Примером могут послужить CAST, DES, IDEA, RC5 и другие системы.

К традиционным методам шифрования относят такие шифры как шифр замены (простой и сложной), шифр перестановки, а также всевозможные их комбинации. В шифрах перестановок основой является перестановка различных сим-

волов. В шифрах простой замены основа – замена одних символов другими, но из этого же алфавита, а в случаях сложной замены для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. [2]

Асимметричные криптографические системы или системы с открытым ключом предполагают, что имеется публичный ключ, который пользователи могут использовать для шифрования. Однако он не может использоваться для расшифрования сообщения. Для этой цели используется второй ключ (уже секретный). К самым распространённым ассиметричным алгоритмам относятся RSA, Elgamal, LUC и другие.

К ряду требований к криптосистемам можно отнести:

– Криптосистема должна быть проста в применении.

– Для расшифровки зашифрованного сообщения необходимо наличие ключа.

– Независимо от того, какой ключ из многообразия будет выбран, должна быть обеспечена надёжная защита информации.

– Шифр должен колоссально меняться даже при малейших изменениях ключа.

– Длина исходного текста не должна отличаться от длины шифротекста.

– На надёжность защиты сообщения не должно влиять знание механизма шифрования. [3]

Увеличение роли информационных технологий в быстроразвивающемся мире привело к тому, что информационная безопасность стала ключевой целью современного общества. Столь быстрое развитие в сфере технологий побуждает к поиску новых методов защиты информации. Криптография как наука ещё не достигла своего пика, поэтому мы можем ожидать дальнейшего развития данного направления.

Литература

1. В. И. Коржик, В.А. Яковлев. Основы криптографии: Учебное пособие / Санкт-Петербург, ИЦ Интермедия, 2016.

2. В.Ф. Голиков, А.В. Курилович. Криптографическая защита информации в телекоммуникационных системах: Учебно-методическое пособие/ Минск, 2006.

3. И.А. Мурашко. Защита компьютерной информации: Конспект лекций / Гомель, 2014.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ЛОГИСТИЧЕСКИХ КОНЦЕПЦИЙ И УПРАВЛЕНИЕ РИСКАМИ В ТАМОЖЕННОМ ДЕЛЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Кильчицкая А.А., Шкробова М.М.
Научный руководитель: ст. преподаватель Лабкович О.Н.
Белорусский национальный технический университет

Таможенная служба Республики Беларусь выполняет важную задачу в регулировании внешней торговли страны. Ее основной задачей является обеспечение соблюдения мер таможенно-тарифного регулирования и создание условий, способствующих ускорению товарооборота через таможенную границу [1].

Таможенная служба Республики Беларусь представляет собой макросистему (взаимодействие с участниками внешнеэкономической деятельности) и множество внутренних микросистем (характерны внутренние связи по иерархической структуре и на горизонтальном уровне).

Как любой макросистеме для эффективной работы необходима логистизация процессов — организация управления движением материальных, финансовых, информационных и других видов потоков. Помочь в управлении логистическими процессами могут концепции управления цепями поставок — Supply Chain Management (SCM).

Таможенные органы Республики Беларусь признают важность применения концепций управления цепями поставок и организации использования процесса таможенными органами, хотя считают, что отсутствует движение товара и его дистрибьюции до покупателя. В последнее время остро встала необходимость применения этих концепций в связи с вступлением в Евразийский экономический союз (ЕАЭС) и внедрением инновационных технологий и систем в деятельность таможенных органов [2].

В работе таможенных органов нет четкой цепи движения товара, поэтому применение одной логистической концепции к каждому процессу невозможно, но применение отдельных частей от разных концепций возможно и приносит положительные результаты.

Информационные потоки и информационные технологии, осуществляющие движение потоков, являются важными в осуществлении таможенной и логистической деятельности.

С точки зрения логистики при перемещении экспортно-импортных товарных потоков через таможенную границу ведущую роль играют потоки таможенных процедур, которые связаны с реализацией таможенных режимов. Таможенная логистическая система имеет каналы входа и выхода. Как и в таможенном деле Республики Беларусь, каналы входа и выхода экспортно-импортных товарных потоков выступают таможенные процедуры, так как они устанавливают порядок