noted. It points to the need for an optimal combination of classical and innovative teaching methods
Key words: quality and level of knowledge, innovative methods, computer technologies, educational process

УДК 004.056.55

ФОРМИРОВАНИЕ ТЕМАТИКИ ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Кутьин М.К., Дубовик А.А.
Военная академия Республики Беларусь

Аннотация. В статье рассматривается формирование тематики учебной дисциплины «Криптографическая защита информации» в интересах подготовки специалистов по противодействию использования информационно-коммуникационных технологий в противоправных целях в условиях многообразия предметной области при ограниченном объеме учебного времени.
Ключевые слова: криптографическая защита информации, шифрование, аутентификация, протокол, учебная дисциплина.

В настоящее время в условиях динамично развивающихся информационно-коммуникационных технологий особую актуальность приобретают две противоположных по целям, но находящихся в постоянном взаимосвязанном развитии, области знаний – защита информации и вскрытие информации.

Все возрастающее значение защиты информации, циркулирующей в различных каналах связи, в системах управления, обуславливается тем, что кибератакам, взлому серверов, вмешательству в функционирование систем управления в настоящее время придается статус элементов гибридной войны. Последствия кибератак для государств могут оказаться много серьезнее, чем последствия силового военного воздействия. Здесь в качестве возможных последствий необходимо рассматривать финансовый и энергетический кризисы, управленческий хаос, транспортный коллапс и другие.

Непрерывно совершенствующиеся технологии защиты информации используются как во благо общества, так и в противоправных целях, когда общедоступные защищенные каналы связи применяются террористами для передачи преступной информации. Именно в связи с этим, в целях предотвращения преступных замыслов возникает насущная необходимость вскрытия защищенной информации. Это обуславливает непрерывное развитие и совершенствование технологий вскрытия защищенной информации.

Защиту информации и вскрытие информации можно рассматривать как обширные области научных знаний, применение которых требует подготовки специалистов с высокой квалификацией. С другой стороны, защиту информации и вскрытие информации можно рассматривать как философские категории единство и борьба противоположностей.

В связи с этим, очевидным становится тезис о том, что при подготовке специалистов по вскрытию информации необходимо глубокое изучение технологий защиты информации.

В настоящее время в области защиты информации выделяют три основных направления:

организационные мероприятия по защите информации;

аппаратные средства и способы защиты информации;

криптографическая защита информации (КЗИ).

Наибольшую эффективность, максимальный вклад в защиту информации привносят криптографические методы защиты. Именно поэтому, в учебных планах подготовки специалистов по защите информации в различных ВУЗах обязательно

фигурирует дисциплина «Криптографическая защита информации» или «Криптографические методы защиты информации».

Опыт применения криптографии составляет уже несколько веков. За это время разработаны десятки методов КЗИ. Использование компьютерных технологий позволило вывести теорию КЗИ совершенно на новый виток развития и совершенства.

Высоконаучная теория и многообразие методов КЗИ требуют аргументированного, взвешенного подхода к наполнению содержания учебной дисциплины особенно в условиях существенно ограниченного бюджета времени. Знакомство с доступными типовыми учебными программами ВУЗов Российской Федерации и Республики Беларусь по данным дисциплинам свидетельствуют о различных подходах к построению дисциплин. При этом акценты расставляются на различные составляющие содержания дисциплин. В ряде программ главный упор делается на теоретические основы и отдельные современные методы защиты информации. В других программах рассматривается теория защиты информации, определенное внимание уделяется историческим методам защиты с акцентом на небольшое количество современных методов.

На взгляд авторов, каждый из существующих подходов имеет право на существование, поскольку реализует вполне определенные цели и задачи, обусловленные спецификой специальности и специализации.

При формировании тематики дисциплины «Криптографическая защита информации» в интересах подготовки специалистов по противодействию использования информационно-коммуникационных технологий в противоправных целях необходимо учитывать следующие требования:

обучаемые должны овладеть теорией КЗИ, что позволит им в дальнейшем самостоятельно изучать новые и перспективные методы КЗИ;

обучаемые должны изучить исторические методы КЗИ для понимания диалектики развития методов защиты и вскрытия информации;

обучаемые должны быть ознакомлены с методами КЗИ, которые имеют широкую программную реализацию на языках программирования, используемых при разработке приложений для основных операционных систем (ОС) компьютеров, смартфонах и т.п.;

обучаемые должны изучить современные методы КЗИ, применяемые для защищенной передачи сообщений наиболее популярными мессенджерами.

При отборе для изучения исторических методов КЗИ необходимо руководствоваться следующими основными тезисами:

методы КЗИ должны демонстрировать диалектику совершенствования защиты информации и способствовать пониманию современных методов;

необходимо включать в тематику изучения те исторические методы, которые по сути стали частью современных.

Исходя их данных тезисов в тематику дисциплины целесообразно включить шифры простой замены (например, шифр Цезаря), полиалфавитные шифры (шифр Гронсфильда и (или) Виженера), а также шифр Тритемиуса, который можно рассматривать в качестве переходного от исторических шифров к современным.

В настоящее время к языкам программирования, которые широко применяются при разработке приложений для основных операционных систем, относятся C# (для ОС Windows) и Java (для ОС Android). Два данных языка программирования очень схожи и обладают схожими возможностями, в том числе, и в области применения алгоритмов шифрования. В табл. 1 приведены обобщенные сведения о криптографических примитивах, для применения которых в каждом из языков разработаны специальные конструкции языка.

Таблица 1. Сведения о криптографических примитивах языков программирования

Криптографические примитивы	Языки программирования		
	C++	C#	Java
DES	+	+	+
Rijndael	+	+	+
TripleDES	+	+	+
Diffie-Hellman	+	+	+
AES	+	+	+
SHA-512	+	+	+
HMAC-SHA-512	+	+	+
ElGamal	-	-	+
RSA	+	+	+

Обзор криптографических примитивов языков программирования C++, C# и Java свидетельствует о примерной равнозначности их возможностей. Можно допустить небольшое преимущество языка Java. В связи с этим при выборе языка программирования для изучения программной реализации методов криптографической защиты информации небольшое предпочтение можно отдать языку Java. Хотя необходимо иметь в виду, что по ключевым примитивам (алгоритмам шифрования, протоколам распределения ключей и аутентификации) возможности языков идентичные.

В рамках подготовки статьи произведен обзор протоколов шифрования применяемых для защиты сообщений в таких известных мессенджерах, как WtatsApp, Signal, Viber, Fasebook Messenger и Telegram. Для обзора использованы источники, доступные в интернете, в том числе официальные сайты мессенджеров. Результаты обзора представлены в табл. 2.

Во всех перечисленных мессенджерах для защиты от несанкционированного доступа применяется, так-называемое, сквозное шифрование E2EE (End-To-End Ecrypton). Разница между данными мессенджерами состоит только в том, что не во всех из них данный режим включается по умолчанию. Смысл режима состоит в том, что доступ к сообщениям имеют только конечные пользователи – отправитель и получатель сообщений. Мессенджер Telegram реализует данный режим только в секретных чатах.

Таблица 2. Сведения о протоколах шифрования, применяемых в наиболее популярных мессенджерах.

Название мессенждера	Протоколы шифрования и используемые примитивы
WhatsApp	X3DH (Curve25519, AES-256, HMAC – SHA256)
Facebook Messenger	X3DH (Curve25519, AES-256, HMAC – SHA256)
Telegram	DH (AES, RSA)
Signal	X3DH (Curve25519, AES-256, HMAC – SHA256)
Viber	X3DH (Curve25519, AES-256, HMAC – SHA256)

Протоколы шифрования в мессенджерах WtatsApp, Signal, Viber, Fasebook Messenger идентичны, так как разрабатывались одной и той же компанией Open Whisper Systems. Протокол шифрования получил название Triple Diffie-Hellman (X3DH) и использует для шифрования и аутентификации примитивы Curve25519, AES-256, HMAC – SHA256 [1].

В мессенджере Telegram пользуются собственным протоколом шифрования. Для распределения ключей применяется протокол распределения ключей Диффи -– Хеллмана (Diffie – Hellman, DH), для шифрования - алгоритм AES и для взаимной аутентификации клиента и сервера используется протокол, основанный на алгоритме RSA [2].

По результатам обзора наиболее популярных мессенджеров можно сделать вывод, о том, что при изучении данной предметной области с точки зрения познания сути шифрования, применяемого в мессенджерах, наибольший интерес представляют такие

примитивы, как алгоритм AES, протокол распределения ключей Диффи – Хеллмана и алгоритмы аутентификации на основе RSA и HMAC – SHA256.

Список литературы

1. WhatsApp Encryption Overview Technical white paper [Электронный ресурс]. // Официальный сайт WhatsApp. URL: https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

2. MTProto Mobil Protocol = Мобильный протокол MTProto [Электронный ресурс]. // Официальный сайт Telegram. URL: http://core.telegram.org/mtproto.

FORMATION OF DISCIPLINE THEMES "CRYPTOGRAPHIC PROTECTION OF INFORMATION"

Kutin M.K., Dubovik A.A.

Military Academy of the Republic of Belarus

Annotation. The article discusses the formation of the subject matter of the discipline “Cryptographic Information Protection” in the interests of training specialists in counteracting the use of information and communication technologies for illegal purposes in a variety of subject areas with a limited amount of study time.

Keywords: cryptographic information protection, encryption, authentication, protocol, academic discipline.

УДК 378.147:811

ПОВЫШЕНИЕ МОТИВАЦИИ К ИЗУЧЕНИЮ ИНОСТРАННОГО ЯЗЫКА В КОНТЕКСТЕ АКАДЕМИЧЕСКОЙ МОБИЛЬНОСТИ

Кушнерова С.Е., Юшкевич Е.В.

Белорусский государственный университет информатики и радиоэлектроники

Аннотация. Данная статья посвящена исследованию академической мобильности и проблеме повышения мотивации к изучению иностранного языка. Представлены различные взгляды на определение академической мобильности. Подчеркивается важность изучения иностранного языка, и рассматриваются виды мотивации и ее взаимосвязь с процессом обучения. Определены возможные способы повышения мотивации, а также факторы, которые необходимо учитывать при обучении иностранному языку.

Ключевые слова: академическая мобильность, мотивация, иностранный язык, процесс обучения, международное сотрудничество.

Интеграция, происходящая во всех сферах человеческой деятельности, касается также системы высшего образования. В настоящее время создается единое образовательное пространство, которое предполагает увеличение обмена между странами в области науки и образования. Это способствует расширению и укреплению межнационального сотрудничества в этой сфере, усилению конкурентоспособности национальных систем образования [1]. Нет сомнения, что академическая мобильность является важным направлением вхождения страны в международное образовательное пространство, а также она способствует повышению качества образования.

Однозначного определения термина “академическая мобильность“ не существует. Авторы ряда научных публикаций объясняют это понятие по - разному. Некоторые определяют академическую мобильность как возможность для студентов, преподавателей перемещаться из одного вуза в другой с целью обмена опытом. Другие, например Н.С. Бринев и Р.А.Чуянов полагают, что академическая мобильность – это период обучения студента в стране, гражданином которой он не является. Этот период ограничен по времени и подразумевает возвращение студента в свою страну по завершении обучения за рубежом [2]. В. И. Богословский и С. А. Писарева считают, что явление академической мобильности многообразно и может классифицироваться по разным основаниям: