С. В. Запечников

ОПЫТ ПРИМЕНЕНИЯ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ КРИПТОЛОГИИ

Введение

По определению [1], *дистанционное обучение* — взаимодействие учителя и учащихся между собой на расстоянии, отражающее все присущие учебному процессу компоненты (цели, содержание, методы, организационные формы, средства обучения) и реализуемое специфичными средствами интернет-технологий или другими средствами, предусматривающими интерактивность.

Всестороннее развитие технологий дистанционного обучения — одна из общемировых тенденций, которая находит широкую поддержку со стороны практически всех университетов, занимающих высокие места в мировых рейтингах: Times Higher Education (THE), Quacquarelli Symonds (QS) World University Rankings, Шанхайском рейтинге и др. Не обошла стороной эта тенденция и преподавание дисциплин в сфере информационной безопасности и криптологии. Однако широкое внедрение дистанционных образовательных технологий при обучении криптологии, которое мы наблюдаем сегодня, не только обусловлено «стихийными» общемировыми тенденциями, но и подготовлено рядом объективных условий, рассматриваемых ниже.

1. Особенности преподавания криптологии в современных условиях

За последние два десятилетия заметно расширилась проблемная область криптологии, возник целый ряд новых областей ее применения и соответствующий им новый научно-методический аппарат. Одновременно наблюдается стабилизация (или даже некоторое ослабление) интереса ученых и практиков к определенным классическим разделам криптологии или относительно новым разделам, до того динамично развивавшимся. Такие бурные изменения обусловлены, с одной стороны, стремительным развитием ИТ и возрастающими потребностями общества в обеспечении безопасности при их реализации, а с другой стороны, новыми научными открытиями в криптологии и смежных областях прикладной математики. Перед университетами, ведущими преподавание криптологических дисциплин, возникла задача адекватного отражения в учебных программах и преподавательской практике неординарных изменений, происходящих в сфере компьютерных наук в целом и криптологии в частности.

В последние годы во всем мире наблюдается неуклонный и стремительный рост числа научных публикаций в области криптологии. Наглядным свидетельством этому служит статистика публикаций (рис. 1) в электронном архиве препринтов Международной ассоциации криптологических исследований IACR [2]. Кроме того, нельзя не учитывать тот факт, что с появлением поисковых сервисов в сети Интернет (Google, Yahoo!, «Яндекс» и др.), электронных энциклопедий (Wikipedia), архивов электронных публикаций и препринтов (CiteSeer, IEEExplore, eprint.iacr.org и др.) принципиально изменились возможности поиска научно-технической информации. Как показывает практика, эти сервисы активно используются и студентами, и преподавателями, поэтому можно быть уверенными в том, что в абсолютном большинстве случаев и преподаватель, и учащийся предпочтет найти интересующий его термин, статью, книгу или описание алгоритма, протокола, метода и т. д. именно при помощи поискового сервиса.

В условиях такого «информационного взрыва» принципиально меняется роль преподавателя. В прошлом он был чуть ли не единственным доступным учащемуся авторитетным источником знаний. Сейчас он скорее превращается в некоторый «фильтр», который должен избавить учащегося от огромного потока лишних, малозначительных или откровенно недостоверных сведений, донося до учащегося лишь высококачественные и системно организованные знания. Задача преподавателя

в этих условиях — так организовать учебный процесс, чтобы максимально повысить эффективность усвоения знаний и приобретения необходимых компетенций учащимися.

Рис. 1. Статистика публикаций в электронном архиве IACR

2. Два сценария применения дистанционных образовательных технологий

Поскольку сама криптология в современных условиях давно уже стала частью информатики (computer science), роль ИТ в обучении криптологическим дисциплинам двойственна: они являются одновременно и предметом изучения, и инструментом организации учебного процесса. Среди таких инструментальных средств ведущее место принадлежит дистанционным образовательным технологиям.

Дистанционные образовательные технологии за последние годы достаточно четко поделились на два сектора:

- технологии, ориентированные на массовое, «поточное» обучение;
- технологии, ориентированные на индивидуальное, «камерное» обучение.

Технологии первого типа в англоязычных источниках принято называть MOOC — massive open online course, что в переводе означает буквально «массовые открытые онлайн-курсы». Это готовые образовательные продукты, включающие в себя как средства обучения, так и информационные ресурсы, доступные в режиме онлайн потенциально неограниченному числу участников через веб-интерфейс. В дополнение к традиционным курсам участникам таких систем обучения могут быть доступны новые виды образовательных ресурсов: видеоролики, интерактивные наборы задач и заданий по программированию, а также форумы пользователей, позволяющие составить своеобразное сообщество студентов, профессоров и преподавателей, задействованных в учебном процессе [3].

Идея MOOC наиболее полно реализуется в сетях дистанционного образования (СДО), доступных через веб-порталы, на которых собраны большие тематические подборки учебных курсов по различным предметным областям. В таблице 1 приведены характеристики наиболее известных и популярных СДО.

СДО отличаются высоким качеством предоставляемых образовательных ресурсов и показывают существенный рост количества доступных учебных курсов. Число слушателей наиболее успешных курсов измеряется десятками и сотнями тысяч человек по всему миру. Так, например, в сети Coursera рекорд принадлежит курсу «Искусственный интеллект», на который по всему миру записалось свыше 180 000 человек одновременно. Как правило, будучи однажды «поставлены на поток», в дальнейшем такие курсы периодически повторяются. Ориентация на столь многочисленную аудиторию определяет характерные черты MOOC:

- отсутствие обратной связи слушателей с преподавателем в режиме онлайн во время проведения занятий (ведущая форма занятий — видеолекции);

- автоматизация проверки выполнения домашних заданий и долгосрочных проектов: контроль знаний проводится либо путем выбора правильных ответов на поставленные задачи и вопросы, либо путем заполнения интерактивных форм с автоматической проверкой форматов и значений введенных величин, либо путем взаимной проверки и рецензирования выполненных работ обучающимися.

Таблица 1. Наиболее известные сети дистанционного образования, представленные в Интернете

№ п/п		Адрес в сети Интернет	Учредители	Кол-во доступных курсов		Стоимость обучения, выдача документа о завершении обучения
				По состоянию на ноябрь 2012 г.	По состоянию на декабрь 2013 г.	
1	Coursera	www.coursera.org	Ун-ты Стэнфорд, Принстон, Беркли, Питтсбург, Иллинойс, Торонто, Огайо, Джорджия, Вирджиния	207	553	Бесплатно, по окончании некоторых курсов выдаются сертификаты
2	edX	www.edx.org	Ун-ты Гарвард, Массачусетс, Беркли, с 2013 г. – Ун-т Техаса	9	110	Ресурсы – бесплатно, сертификаты – пока бесплатно, в будущем станут платными
3	UM Global Academy	umga.miami.edu	Ун-т Майами	Middle school – 39, High school – 91	Middle school – 39, High school – 73	Стоимость регистрации $70 для доступа ко всем ресурсам и курсам
4	Udacity	www.udacity.com	Частная компания	18	33	Бесплатно
5	MIT Open Coursware	ocw.mit.edu	Массачусетский технологический институт	2100	2150	Ресурсы – бесплатно, сертификаты не выдаются

За редким исключением, рабочий язык всех курсов – английский. Практически во всех СДО, перечисленных в таблице 1, представлены курсы по криптологическим дисциплинам: примерами являются курсы “Cryptography I” и “Cryptography II”, которые проводит профессор Стэнфордского университета Dan Boneh в сети Coursera, курс “Computer Security”, проводимый совместно Стэнфордским университетом и Калифорнийским университетом в Беркли (США) в той же сети, курс “Applied Cryptography”, который проводит профессор Университета Вирджинии (США) David Evans, несколько курсов по сетевой безопасности и криптографии (как общего характера, так и специализированных) Массачусетского технологического института (США)

в сети MIT Open Courseware. В совокупности представленные в СДО курсы охватывают все ступени обучения: от undergraduate до postgraduate, то есть от бакалавриата до аспирантуры.

По мнению автора статьи, очевидные достоинства образовательных курсов, представленных в сетях дистанционного образования: их высокое качество и минимальные затраты на обучение — позволяют рекомендовать их для самообразования как профессорско-преподавательскому составу российских вузов, так и студентам, обучающимся по программам магистратуры и специалитета.

Однако технологии, ориентированные на массовое обучение, не исчерпываются СДО. Как уже отмечалось, в их основе лежат веб-технологии. Поэтому создание многофункциональных веб-сайтов, помогающих поддерживать учебный процесс и организовывать различные формы взаимодействия между преподавателями и учащимися, также способно принести немало пользы.

Технологии второго типа по существу представляют собой разные виды телеконференций с одним или несколькими ведущими и небольшим числом участников, активно включенных в процесс взаимодействия с ведущими. За ними в последнее время закрепилось специальное название «вебинары», являющееся калькой английского слова "webinar", полученного соединением слов "web" и "seminar", то есть семинар, проводимый с использованием веб-технологий (онлайн-семинар, веб-конференция). Действительно, всем участникам телеконференции необходимо либо установить на своих компьютерах специальное программное обеспечение, либо использовать специальные веб-сервисы, предоставляемые провайдерами в сети Интернет. Пожалуй, самыми известными примерами являются сервисы Cisco WebEx, Citrix Online, Microsoft Office Live Meeting. Вместе с тем число провайдеров веб-конференций (как зарубежных, так и российских) увеличивается с каждым днем.

Как показывает практика, веб-конференции хорошо подходят для проведения лекционных и семинарских занятий по самым различным дисциплинам, в частности, по широкому спектру дисциплин в сфере информационных технологий. В настоящее время многие российские вузы и учебные центры также реализуют учебные курсы по направлению «Информационная безопасность» в форме веб-конференций.

3. Авторский опыт применения дистанционных образовательных технологий, ориентированных на массовое обучение

Автором настоящей статьи в 2013 г. создан и администрируется сайт поддержки учебного процесса по криптологическим дисциплинам, доступный по адресу: http://cryptowiki.net. Сайт используется в качестве справочно-информационного ресурса для специалистов в области криптографии и для выполнения всех видов домашних заданий и самостоятельной работы студентов при изучении дисциплин «Криптографические протоколы и стандарты», «Криптография в банковском деле». На этом же сайте размещены материалы для самостоятельной работы студентов, описание правил ведения рейтинговой системы учета успеваемости студентов, видеозаписи вебинаров, ранее проведенных автором.

Сайт функционирует на базе коммерчески доступного хостинга на платформе Windows, на котором установлена свободно распространяемая система управления контентом («движок») MediaWiki версии BitNami. Интерфейс системы подобен хорошо известному абсолютному большинству пользователей интерфейсу «Википедии» (рис. 2).

Центральное место на сайте занимает справочно-информационная система, названная «Энциклопедией теоретической и прикладной криптографии». Это создаваемый совместными усилиями преподавателя и студентов обширный информационный ресурс, включающий в себя все виды контента, доступные для размещения на сайте: текстовые и графические материалы, видеоролики, демонстрационные программы, математические выражения, листинги фрагментов программ и др. Справочно-информационная система состоит из более чем 55 содержательных разделов, каждый из которых посвящен одному из крупных направлений современной

криптографии, объединенных в две части: «Основы криптографии (Криптографические примитивы)» и «Приложения криптографии (Криптографические протоколы)». Контент всех разделов дублируется на русском и английском языках.

Выполнение заданий, взаимное их рецензирование студентами и комментирование преподавателями на страницах сайта создает открытую и прозрачную для всех участников учебного процесса среду, способствует повышению публичности результатов работы студентов и объективности оценки их работы преподавателем.

Помимо «Энциклопедии…», на сайте реализована и традиционная для сайтов учебно-методического характера функциональность: информационные материалы, «доска объявлений», дополнительные материалы к лекционным занятиям и пр.

Хотелось бы указать еще на одну модель применения ИТ в обучении криптологическим дисциплинам, обладающую, как представляется, большими потенциальными возможностями. Ни для кого не секрет, что в отечественной высшей школе весьма сильна традиция «теоретизации» (иногда излишней) значительного числа преподаваемых в вузе дисциплин, что в прошлом обуславливалось, прежде всего, ярко выраженной направленностью на массовую подготовку научно-педагогических кадров высшей квалификации. Однако в связи с произошедшими за последние два десятилетия переменами в экономической и социальной жизни нашей страны существенно возрос спрос на освоение студентами практических приемов работы с самыми современными аппаратно-программными средствами, приобретение опыта практической работы по специальности. Лабораторная база многих учебных заведений, да и уровень их финансирования, оказались не готовы к выполнению этих требований.

Вместе с тем во всем мире заметно расширяется применение ПО с открытым исходным кодом (open source software). Условия лицензионных соглашений на такое ПО в подавляющем большинстве случаев разрешают либо полностью свободное его использование для любых целей, либо по крайней мере свободное использование в некоммерческих и образовательных проектах. Отслеживание появления в сети Интернет свободно распространяемого ПО, обладающего большим потенциалом применения при обучении криптологии, и его освоение (в частности, постановка новых лабораторных работ и заданий на производственную практику) позволяют заметно усилить практическую направленность модернизируемых курсов криптологии. Характерными примерами такого ПО могут служить библиотеки криптографических алгоритмов Crypto++, PyCrypto, средство прототипирования криптографических конструкций Charm и многие другие образцы ПО с открытым исходным кодом.

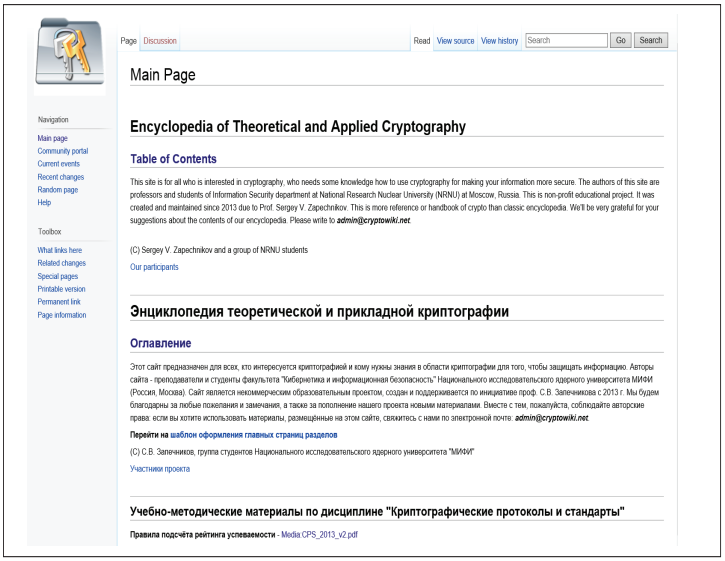

Рис. 2. Главная страница сайта cryptowiki.net

4. Авторский опыт применения дистанционных образовательных технологий, ориентированных на индивидуальное обучение

Дистанционные образовательные технологии, ориентированные на индивидуальное обучение, хорошо подходят для организации как краткосрочных, так и длительных образовательных курсов в тех случаях, когда по каким-либо причинам невозможно регулярное очное общение между преподавателем и учащимися, например, при проведении курсов повышения квалификации и профессиональной переподготовки.

В таблице 2 приведена разработанная автором программа из нескольких блоков криптологических дисциплин, которая является составной частью 540-часовой программы курсов профессиональной переподготовки по направлению 090900 — «Информационная безопасность». Всю теоретическую (лекционно-семинарскую) часть этих курсов удалось реализовать, применяя упомянутые выше дистанционные образовательные технологии. И только лабораторные модули обучения реализовывались в очной форме: единый блок лабораторных занятий проводился по окончании теоретического обучения.

Таблица 2. Извлечение из программы курса профессиональной переподготовки: блоки криптологических дисциплин

День занятий, количество часов	**Виды занятий (Л — лекция, С — семинар, ПЗ — практические занятия), темы занятий**
Модуль «Основы информационной безопасности и криптографической защиты информации»	
Дистанционное обучение (вебинары)	
1-й день (8 акад. часов)	*Л:* Основы криптографии. Классическая криптография.
	Л: Основы криптографии. Классическая криптография.
	Л: Симметричные криптосистемы: блочные и поточные шифры, режимы шифрования, криптографические генераторы, практические аспекты применения шифров.
	Л: Симметричные криптосистемы: блочные и поточные шифры, режимы шифрования, криптографические генераторы, практические аспекты применения шифров.
2-й день (8 акад. часов)	*Л:* Асимметричные криптосистемы: открытое распределение ключей, протокол Диффи — Хеллмана, схемы открытого шифрования, электронная цифровая подпись.
	Л: Асимметричные криптосистемы: открытое распределение ключей, протокол Диффи — Хеллмана, схемы открытого шифрования, электронная цифровая подпись.
	Л: Криптографические хэш-функции и их применение.
	Л: Управление ключами: основы управления ключами, регламентация работы с ключевыми носителями, организационное обеспечение систем криптографической защиты информации.

3-й день (8 акад. часов)	*Л:* Ключевые системы симметричных и асимметричных криптосистем, концепция инфраструктуры открытых ключей (PKI).
	Л: Криптографические протоколы: основные понятия и определения, важнейшие типы криптографических протоколов, примеры. Способы, средства и протоколы криптографической защиты информации, передаваемой по каналам связи.
	Л: Криптографические протоколы: основные понятия и определения, важнейшие типы криптографических протоколов, примеры. Способы, средства и протоколы криптографической защиты информации, передаваемой по каналам связи.
	С: Стандартизация методов и средств криптографической защиты информации (международные и отечественные стандарты).
Модуль «Криптографические методы защиты информации»	
Дистанционное обучение (вебинары)	
1-й день (8 акад. часов)	*Л:* Исторический экскурс по классической криптографии: с древнейших времен до начала XX в.
	С: Выводы из классической криптографии: типы шифров, базовые математические понятия.
	Л: Криптография первой половины XX в.: электромеханические шифровальные машины и их устройство.
	Л: Теория Шеннона и ее значение для развития современной криптографии во второй половине XX в.
2-й день (8 акад. часов)	*Л:* Случайные и псевдослучайные генераторы. Критерии качества криптографических генераторов.
	Л: Конструкции криптографических генераторов случайных и псевдослучайных двоичных последовательностей.
	Л: Определение поточного шифра. Требования к стойкости поточного шифра.
	Л: Конструкции поточных шифров. Примеры. Применение поточных шифров.
3-й день (8 акад. часов)	*Л:* Определение блочного шифра. Требования к стойкости блочного шифра.
	Л: Конструкции блочных шифров: шифры, основанные на петле Фейстеля, примеры.
	Л: Конструкции блочных шифров: шифры, основанные на петле Фейстеля (DES, ГОСТ 28147-89 и др.), их стойкость. Криптоанализ блочных шифров.
	Л: Конструкции блочных шифров: шифры, основанные на алгебраических операциях (на примере AES), и их стойкость.
4-й день (8 акад. часов)	*Л:* Симметричные схемы шифрования. Стойкость симметричных схем шифрования.
	Л: Симметричные схемы аутентификации сообщений на основе блочных шифров.
	Л: Криптографические хэш-функции (бесключевые).
	С: Сравнительная оценка симметричных криптографических алгоритмов.

5-й день (8 акад. часов)	*Л:* Симметричные схемы аутентификации сообщений на основе криптографических хэш-функций.
	Л: Схемы аутентичного шифрования.
	Л: Симметричные криптосхемы с расширенными свойствами и с дополнительной функциональностью.
	Л: Управление ключами симметричных криптосистем.
6-й день (8 акад. часов)	*Л:* Вычислительно сложные задачи, используемые в асимметричной криптографии. Однонаправленные функции.
	Л: Генерация параметров и ключей асимметричных криптосхем.
	Л: Открытое распределение ключей. Протокол Диффи — Хеллмана.
	Л: Арифметические алгоритмы, используемые в асимметричной криптографии.
7-й день (8 акад. часов)	*Л:* Определение схемы открытого шифрования. Стойкость схем открытого шифрования.
	Л: Схемы открытого шифрования на основе однонаправленной функции с потайной дверью (схемы RSA, Рабина и др.).
	Л: Схемы открытого шифрования на основе дискретного логарифмирования (схема Эль-Гамаля и др.).
	С: Сравнительная оценка симметричных шифров и схем открытого шифрования.
8-й день (8 акад. часов)	*Л:* Определение схемы цифровой подписи. Стойкость схем цифровой подписи.
	Л: Схемы цифровой подписи на основе задачи RSA.
	Л: Схемы цифровой подписи на основе задачи дискретного логарифмирования.
	С: Сравнительная оценка симметричных и асимметричных методов аутентификации сообщений.
9-й день (8 акад. часов)	*Л:* Математические основы криптографии на эллиптических кривых.
	Л: Асимметричные криптосхемы на основе математического аппарата эллиптических кривых.
	Л: Асимметричные криптосхемы на основе математического аппарата билинейных спариваний. Перспективы эллиптической криптографии.
	С: Практические аспекты обеспечения стойкости СКЗИ. Характерные ошибки, допускаемые при реализации.
10-й день (4 акад. часа)	*С:* Регулирование разработки и применения СКЗИ в России.
	С: Структура криптосистем. Составление «карты», показывающей взаимосвязь основных разделов традиционной и современной криптографии.
Очное обучение (лабораторные занятия)	
1-й день (9 акад. часов)	*ПЗ:* Стандартные сетевые утилиты. Сетевой сканер Nmap. Анализатор трафика tcpdump.
	ПЗ: Межсетевое экранирование в ОС Linux. Трансляция сетевых адресов.
	ПЗ: Удаленное управление и туннелирование по протоколу SSH. Шифрованные файловые системы.
	ПЗ: Система аутентификации, учета и аудита в ОС Linux.

2-й день (9 акад. часов)	*ПЗ:* Перемешивающие свойства криптографических преобразований. Симметричные криптосистемы.
	ПЗ: Методы криптоанализа. Асимметричные криптосистемы.
Модуль «Безопасность открытых информационных систем»	
Дистанционное обучение (вебинары)	
1-й день (8 акад. часов)	*Л:* Основы конструирования криптографических протоколов.
	Л: Базовые конструкции протоколов аутентификации. Аутентификация по паролю. Аутентификация «запрос — ответ».
	Л: Доказательства с нулевым разглашением знания. Протоколы аутентификации, основанные на доказательствах с нулевым разглашением знания.
	С: Сферы практического применения криптографических протоколов.
2-й день (8 акад. часов)	*Л:* Базовые конструкции протоколов распределения ключей. Основные понятия и определения. Свойства протоколов распределения ключей.
	Л: Протоколы распределения ключей, основанные на симметричных криптографических методах.
	Л: Протоколы распределения ключей, основанные на симметричных криптографических методах.
	Л: Протоколы удаленной аутентификации и механизмы единого входа в систему (single sign-on). Протокол Kerberos.
3-й день (8 акад. часов)	*Л:* Защищенная электронная почта. Спецификация PGP.
	Л: Протоколы обеспечения безопасности сервиса мгновенного обмена сообщений. Протокол Off-the-Record Messaging v3 (OTR).
	Л: Криптографические протоколы в анонимных сетях. Протоколы сети TOR.
	Л: Криптографическая защита систем кооперативного обмена данными (пиринговых сетей).
4-й день (8 акад. часов)	*Л:* Криптографические протоколы для образования защищенных каналов передачи данных. Способы и средства установления защищенных соединений.
	Л: Спецификация SSH.
	Л: Спецификация SSL/TLS.
	Л: Анализ стойкости протоколов SSL/TLS. Уязвимости к атакам, классификация атак.
5-й день (8 акад. часов)	*Л:* Спецификация IPSec.
	Л: Анализ стойкости протоколов IPSec. Уязвимость к атакам, классификация атак.
	Л: Спецификации для беспроводных сетей: WEP, WPA, WPA2, WiMax, LTE: криптографическое ядро протоколов, стойкость и уязвимости, сравнительный анализ.
	С: Обеспечение сетевой безопасности криптографическими методами: сравнительный анализ криптографических методов, средств и протоколов.

6-й день (8 акад. часов)	*Л:* Схемы разделения секрета. Пороговые криптосхемы. Пороговая криптография. Примеры практического применения пороговых схем.
	Л: Обеспечение информационной безопасности распределенных вычислений криптографическими методами. «Задача о византийских генералах». Протокол «византийского соглашения».
	Л: Протоколы обеспечения безопасности доступа к базам данных и облачным хранилищам данных. Атрибутный контроль доступа к шифрованным данным.
	Л: Квантовая криптография. Постквантовая криптография. За пределами постквантовой криптографии. Актуальные направления и нерешенные проблемы криптографии (краткий обзор).
7-й день (4 акад. часа)	*Л+ПЗ:* Библиотеки разработчика СКЗИ, инструментальные средства создания прототипов СКЗИ (краткий обзор). Аппаратные средства поддержки криптографических механизмов. «Экскурсия» по сайтам, полезным для разработчика алгоритмов и программного кода СКЗИ.
	С: Стойкость и уязвимости средств криптографической защиты информации. Криптостойкость и стойкость СКЗИ. Анализ типичных ошибок при реализации.
Очное обучение (лабораторные занятия)	
1-й день (8 акад. часов)	*ПЗ:* Комплексы ФПСУ-IP. Общие сведения о комплексе, аппаратные и программные средства. Инсталляция программного обеспечения комплекса. (4 часа)
	ПЗ: Управление администраторами. Управление начальной загрузкой. Организация работы ключевой системы. Настройка сетевых адаптеров. Установка дополнений и новых версий. Режимы отображения при запущенном комплексе. (4 часа)
2-й день (8 акад. часов)	*ПЗ:* Комплексы ФПСУ-IP. Эксплуатация комплекса. Настройка портов. Групповые политики. (4 часа)
	ПЗ: Удаленный администратор — установка, конфигурирование, администрирование. (4 часа)
3-й день (8 акад. часов)	*ПЗ:* Взаимодействие комплекса с сетевым оборудованием. Комплексы ФПСУ-IP/Клиент. Центр Генерации Ключей Клиентов. Устройство VPN-key. (4 часа)
	ПЗ: Инсталляция и настройка клиента локально и на комплексе. Взаимодействие со стандартными межсетевыми экранами (Kerio WinRoute firewall, MS ISA Client). (4 часа)
Модуль «Информационная безопасность автоматизированных банковских систем»	
Дистанционное обучение (вебинары)	
1-й день (8 акад. часов)	*Л:* Криптография в банковском деле: отечественный опыт. Основные направления применения криптографии в АБС. «Финансовая криптография». Нормативно-правовые и нормативно-технические основы криптографической защиты информации в организациях банковской системы РФ.
	Л: Требования стандартов Банка России по обеспечению информационной безопасности в организациях банковской системы РФ криптографическими средствами.
	Л: Формы безналичных расчетов в РФ и в международной практике. Унифицированные форматы электронных банковских сообщений в РФ и их защита криптографическими методами.

	Л: Унифицированные форматы электронных банковских сообщений в системе международного финансового обмена SWIFT и их защита криптографическими методами.
2-й день (8 акад. часов)	*Л:* Системы межбанковских расчетов: обеспечение информационной безопасности. Криптографическая защита систем дистанционного банковского обслуживания (ДБО).
	Л: Криптографическая защита систем розничных платежей, в том числе систем «мгновенных» платежей.
	Л: Системы онлайн-платежей в Интернете, «электронные кошельки», «электронные деньги», их криптографическая защита.
	Л: Система «криптовалюты» BitCoin, дискуссия о ее безопасности и перспективах.
3-й день (8 акад. часов)	*Л:* Пластиковые карты и криптографические особенности их применения в банковском деле. Стандарты ISO/IEC.
	Л: Системы платежей по банковским картам: обеспечение информационной безопасности. Спецификация SET. Спецификация 3D-Secure.
	Л+ПЗ: Комплекс методов и средств криптографической защиты информации в современных защищенных информационных технологиях (ПЗ на основе электронного справочно-энциклопедического пособия) (начало).
4-й день (4 акад. часа)	*Л+ПЗ:* Комплекс методов и средств криптографической защиты информации в современных защищенных информационных технологиях (ПЗ на основе электронного справочно-энциклопедического пособия) (окончание).
Очное обучение (лабораторные занятия)	
1-й день (8 акад. часов)	*ПЗ:* Криптографические средства для шифрования данных на дисках. Защищенный документооборот. (4 часа)
	ПЗ: Развертывание MS Certificate Authority. Аутентификация с помощью сертификатов. (4 часа)
2-й день (8 акад. часов)	*ПЗ:* Аутентификация. Цели и задачи. Типы, методы аутентификации и их особенности. Использование технологии аутентификации для корпоративных сетей. Анализ существующих угроз безопасности относительно процедуры аутентификации. Идентификаторы Rutoken. Назначение. Технические характеристики. Архитектура Rutoken.
	ПЗ: Двухфакторная идентификация. Использование технологии двухфакторной идентификации на базе идентификаторов Rutoken RF. Архитектура Rutoken. Аппаратная платформа, комплекс программного обеспечения Rutoken.
	ПЗ: Установка и администрирование идентификатора. Утилита обслуживания Rutoken. Утилита администрирования Rutoken. Браузер сертификатов. Централизованная интеграция идентификатора Rutoken в домен Active Directory. Использование групповых политик в процессе интеграции и централизованного управления.
	ПЗ: Использование идентификаторов Rutoken для безопасного хранения цифровых сертификатов и закрытых ключей ЭЦП и шифрования. Интеграция идентификатора Rutoken в качестве защищенного хранилища сертификатов

	с Microsoft Certificate Services. Реализация защищенной электронной почты с использованием идентификатора Rutoken. Интеграция идентификатора Rutoken с продуктами компании «КриптоПро». Построение защищенного документооборота, соответствующего российским стандартам.
	ПЗ: Криптографические средства для шифрования данных на дисках. Защищенный документооборот.

Опыт реализации этой программы наглядно демонстрирует весь потенциал дистанционных образовательных технологий. В данном случае удалось реализовать полный курс криптологии: от введения в предмет для начинающих до расширенного уровня знаний, умений и навыков, достаточного для владения приемами разработки программного и аппаратного обеспечения новых СКЗИ. Как показывает опыт, проведение занятий в форме веб-конференций не только является вполне адекватной заменой традиционным лекциям «у доски», но и существенно повышает интенсивность подачи материала слушателям и, тем самым, эффективность учебного процесса в целом.

Заключение

Подводя итоги обсуждению опыта применения дистанционных образовательных технологий при обучении криптологии, отметим следующее.

1. Анализ существующих дистанционных образовательных технологий и личный опыт автора по их применению при обучении криптологии свидетельствуют о том, что дистанционные образовательные технологии позволяют существенным образом модернизировать формы проведения всех видов учебных занятий: лекционных, семинарских, лабораторных. Основным позитивным эффектом при этом является повышение эффективности основного учебного процесса, а также повышение удобства взаимодействия преподавателей и учащихся при выполнении домашних заданий, курсовых проектов, решении организационных вопросов и освоении факультативных разделов дисциплин.

2. Две ярко выраженные современные тенденции развития дистанционных образовательных технологий — сети дистанционного образования (а также примыкающие к ним многофункциональные веб-ресурсы, рассчитанные на более узкую аудиторию) и веб-конференции (вебинары). Сети дистанционного образования являются наиболее ярким проявлением складывающегося глобального образовательного пространства и глобальной конкуренции ведущих мировых университетов в сфере образовательных процессов. Веб-конференции — наиболее эффективная форма организации занятий для небольших групп учащихся. Дистанционные образовательные технологии, реализующие оба подхода, в равной мере применимы при обучении криптологическим дисциплинам.

3. Приобретенный опыт применения дистанционных образовательных технологий при обучении криптологии может быть распространен на другие специальные дисциплины, преподаваемые студентам, слушателям курсов повышения квалификации и курсов переподготовки, обучающимся по направлению «Информационная безопасность», а также на управление процессом выполнения студентами учебно- и научно-исследовательских работ, практик, выпускных квалификационных работ.

СПИСОК ЛИТЕРАТУРЫ:

1. «Термины и определения дистанционного обучения» [Электронный ресурс] / Лаборатория дистанционного обучения Российской академии образования. URL: http://distant.ioso.ru/do/termin.htm (дата обращения: 13.12.2013).
2. Cryptology ePrint Archive [Электронный ресурс]. URL: http://eprint.iacr.org (дата обращения 13.12.2013).
3. *Waldrop M.* Massive Open Online Courses, aka MOOCs, Transform Higher Education and Science. Scientific American. April 2013. URL: http://www.scientificamerican.com/article.cfm?id=massive-open-online-courses-transform-higher-education-and-science (дата обращения: 14.12.2013).