совершенствования среднего специального, высшего и послевузовского образования, как нашей стране, так и за ее пределами.

1. Абасова, С.Э. Применение новых информационных технологий в дистанционном обучении / С.Э. Абасова, С.Г. Абдуллаев // Дистанционное и виртуальное обучение. – 2011. – № 11
2. Браженская Е. О. Плюсы и минусы информационных технологий // Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. XV междунар. студ. науч.-практ. конф. № 15. / [Электронный ресурс]. - Режим доступа: [http://sibac.info/archive/technic/9\(12\).pdf](http://sibac.info/archive/technic/9(12).pdf) (дата обращения: 25.11.2017)
3. Ирзаев Г.Х. Модель интегрированной информационно-коммуникационной среды поддержки учебного процесса в вузе // Современные научные исследования и инновации. 2014. № 10-1 (42). С. 68-70.
4. Информатизация общего среднего образования: науч.-метод. пособие / под ред. Д. Ш. Матросова. - М. Педагогическое общество России, 2004. -384 с.
5. Инновационные технологии в образовании / Под ред. Абылгазиева И.И., Ильина И.В. / Сост. Земцов Д.И. - М.: МАКС Пресс, 2011. -141 с.
6. Ирзаев Г.Х., Мурадов М.М. Автоматизированная система мониторинга и оценки публикационной активности преподавателя кафедры вуза // Современные научные исследования и инновации. 2014. № 8-1 (40). С. 64-70.
7. Киренберг А.Г., Колесников О.М. Способ построения беспроводного интернет-канала в условиях малоэтажного жилого сектора // Информационно-телекоммуникационные системы и технологии (ИТСиТ-2014): Материалы Всероссийской научно-практической конференции, г. Кемерово, 16-17 октября 2014 г.; Кузбас. гос. техн. ун-т им. Т.Ф. Горбачева. – Кемерово, 2014.
8. Киренберг А.Г., Колесников О.М. Проблема подключения к интернету малоэтажного жилого сектора России и возможный способ ее решения // Журнал «Вестник Кузбасского государственного технического университета», №1 (107), 2015. - Кузбас. гос.техн. ун-т им. Т.Ф. Горбачева. – Кемерово, 2015.

Кузнецов Е.М., Апрелева А.Д.

Использование основ криптографии в образовательном процессе

*Поволжский государственный университет телекоммуникаций и информатики
Самарский социально-педагогический колледж
(Россия, Самара)*

doi: 10.18411/lj-28-02-2018-40

idsp: 000001:lj-28-02-2018-40

Аннотация

В статье изложены простые подходы к использованию основ криптографии в образовательном процессе.

Ключевые слова: криптография, исследовательские навыки, инфокоммуникационные технологии.

Применение полного комплекса информационных технологий для гармоничного развития личности в современном обществе и проникновение современных этих технологий в повседневную жизнь каждого человека диктует новые подходы в образовании. Как следствие, даже такие ранее неиспользуемые в образовательном процессе технологии как криптография должны внедряться в данный процесс. И перед техническими науками встает проблема как опосредовать данные достаточно сложные технологии для использования в образовательном процессе с целью повышения исследовательской и познавательной активности обучающихся.

Развития информационных технологий и, особенно в связи с широким распространением Интернета, защита конфиденциальной информации стала одной из актуальнейших задач современности. Ситуация складывается так, что в недалёком будущем знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией. Поэтому вскоре криптография станет «третьей

грамотностью» - по аналогии со «второй грамотностью», как называют владение компьютером и информационными технологиями. Также использование различных гаджетов в повседневной жизни и образовательном процессе поднимает проблему сохранности персональных данных и защиты персональных данных. В связи с этим проблема внедрения криптографии в образовательный процесс наиболее актуальна на современном этапе.

Использование криптографии на сегодняшний день является единственным способом защитить персональные данные [1].

В последние годы почти экспоненциально возрастает использование ресурсов локальных, национального масштаба и даже международных сетей в образовательных учреждениях – в связи с этим проблемы защиты информации в перечисленных сетях требует решения на уровне образовательного процесса [3].

На протяжении всей своей истории человек испытывал потребность в шифровке той или иной информации. Неудивительно, что из этой потребности выросла целая наука — криптография. И если раньше криптография по большей части служила исключительно государственным интересам, то с приходом интернета ее методы стали достоянием частных лиц и широко используются хакерами, борцами за свободу информации и любыми лицами, желающими в той или иной степени зашифровать свои данные в сети [3].

Криптоанализом (от греческого *kryptos* - "скрытый" и *analein* - "ослаблять" или избавлять") называют науку восстановления (дешифрования) открытого текста без доступа к ключу. Хотя история криптоанализа насчитывает многие века, особенно интенсивно эта область знаний начала развиваться с наступлением компьютерной эры [2].

Внедрение методов криптографии в образовательный процесс происходит путем разработки различных упражнений и проектов, разрабатываемых студентами. В зависимости от возраста рассматриваются синхронные ключи для шифрования персональных данных или поиска информации необходимой для создаваемого проекта, или асинхронные ключи шифрования как современный этап развития криптографии. В дальнейшем должно состояться знакомство с будущими методами криптографии на основе квантовых данных или шифрования при помощи квантового компьютера.

Набор таких упражнений или проектов, произведенных с использованием технологии веб-квеста и методов криптографии, разрабатывается в процессе работы группами ученых и студентов в РФ.

Внедрение методов криптографии в образовательный процесс, дает возможность развивать и стимулировать как учебную деятельность, так и познавательный и научно-исследовательский интересы обучающихся, способствует развитию личности обучающегося. Таким образом, на примере формирования формальных и логических основ защиты информации современными методами криптографии происходит слияние процесса обучения с реальной жизнью, то есть социализация и решается проблема защиты персональных данных на уровне методов криптографии каждым студентом.

1. Кузнецов Е.М., Драгина К.Ю. Материалы международной научно-практической молодежной конференции «Интеллектуальный потенциал XXI века» // Мир науки и инноваций № 2 2015 том 2. С. 9-12
2. Кузнецов Е.М., Драгина К.Ю. Использование криптографии в образовании // Научные труды SWorld. 2016. Т. 2. № 44. С. 47-50.
3. Кузнецов Е.М. Проблема использования методов моделирования корпоративных информационно-вычислительных сетей в учебном процессе // Глобальный научный потенциал. 2016. № 3 (60). С. 18-19.