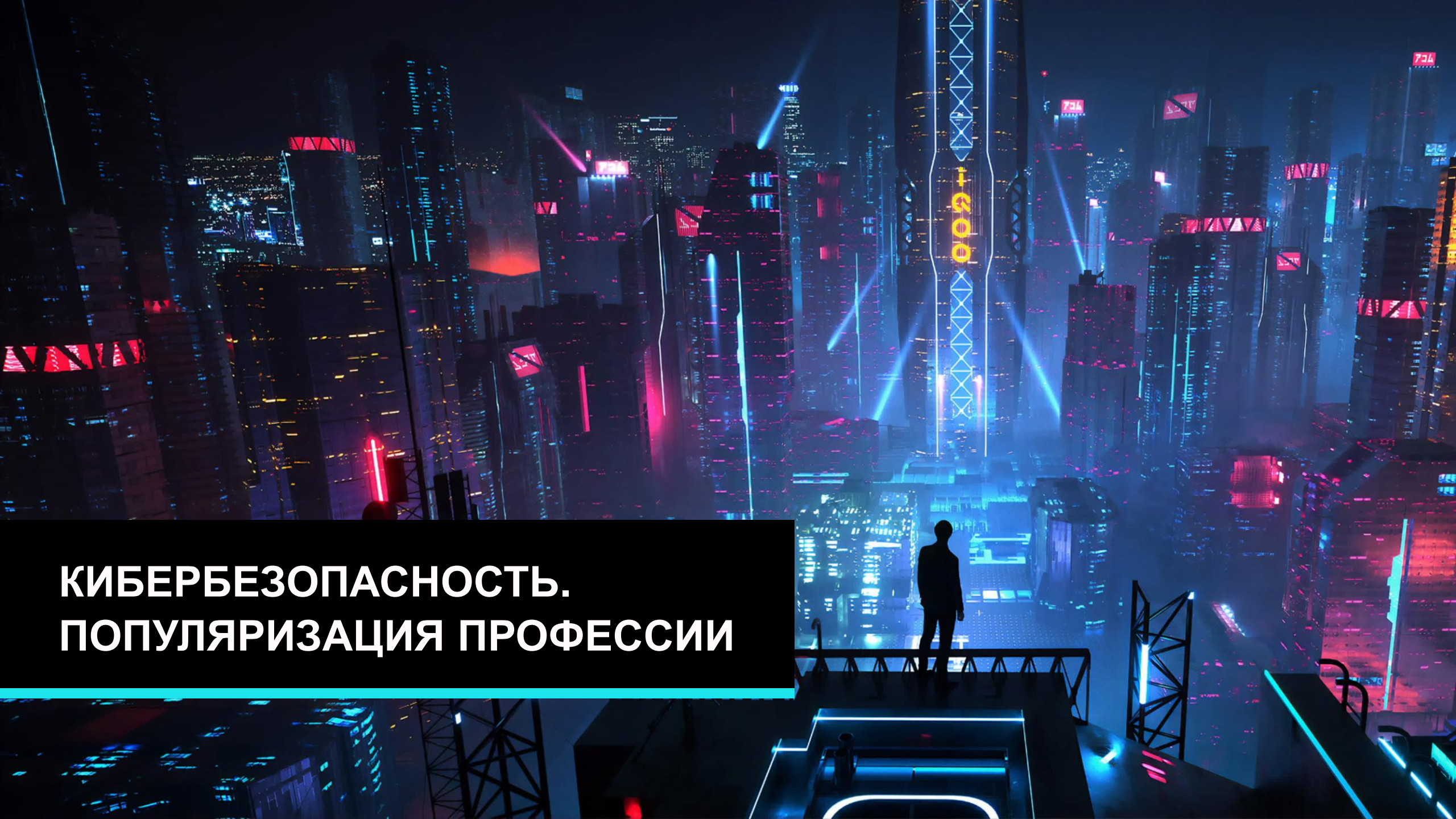


КИБЕРБЕЗОПАСНОСТЬ. ПОПУЛЯРИЗАЦИЯ ПРОФЕССИИ

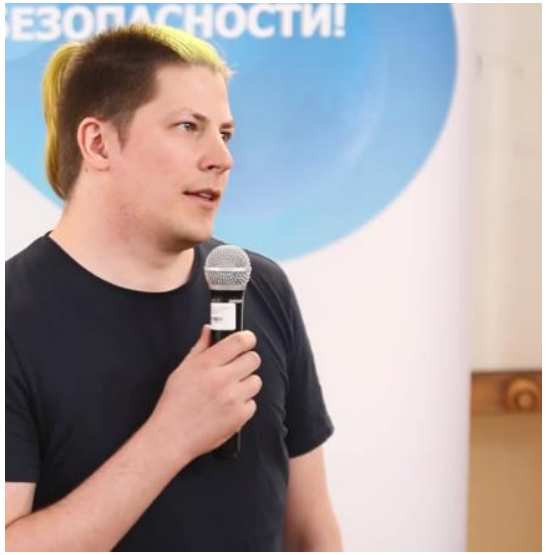
ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

ПОЛИТЕХ
Институт кибербезопасности
и защиты информации

ОЧНАЯ РАБОТА СО ШКОЛЬНОЙ АУДИТОРИЕЙ

Работа со школами

Выставки



Дни открытых дверей

ЛЕТНИЕ ПРАКТИКИ ДЛЯ ФИЗМАТ ШКОЛ

- Исследуем опасности современных технологий
- Проникаем внутрь Android
- Программируем в сфере ИБ
- Проводим сетевую атаку
- Внутри СУБД. Атаки и защита данных
- Исследуем вредоносные программы
- Шифруем vs ломаем!

ДОПОЛНИТЕЛЬНОЕ ОБРАЗОВАНИЕ

Работа с Центром «Сириус» , мастер класс для 9-11 классов «Спрятать на виду»

Работа с «Академией талантов» г. Санкт-Петербурга

ИНТЕРНЕТ-ПРОДВИЖЕНИЕ

Сайт института

Вконтакте: видеоролики, статьи, посты.

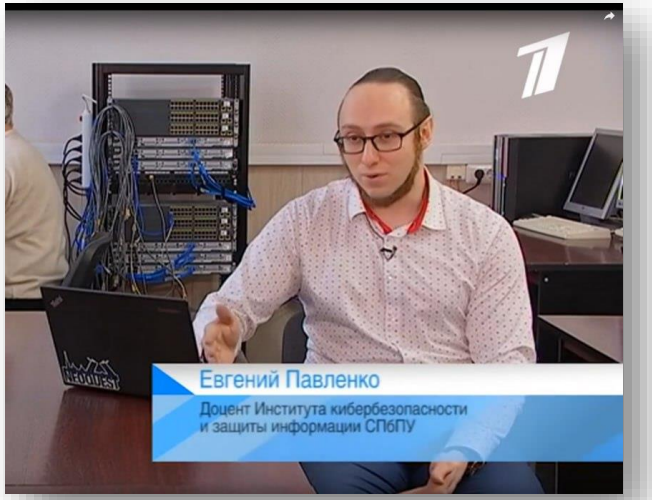
Телеграм-канал: информирование, ответы на вопросы, живое общение с привлечением студентов и преподавателей

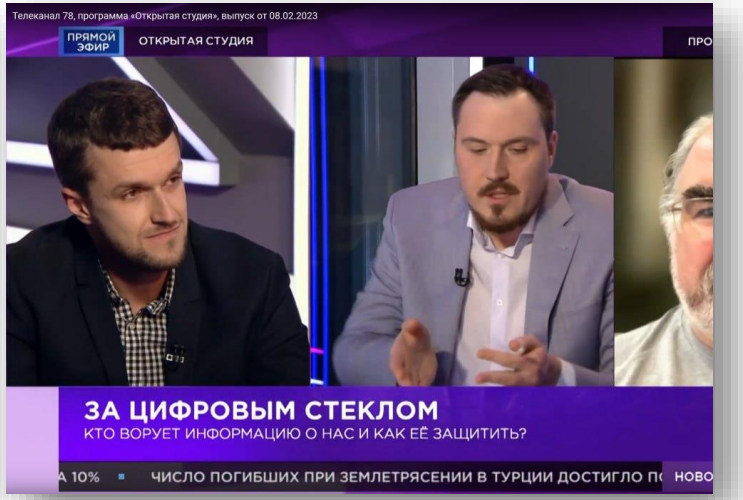
РАБОТА ПО ПОПУЛЯРИЗАЦИИ СО ВЗРОСЛОЙ/СТУДЕНЧЕСКОЙ АУДИТОРИЕЙ

Повышение цифровой грамотности, ликбез по кибербезопасности

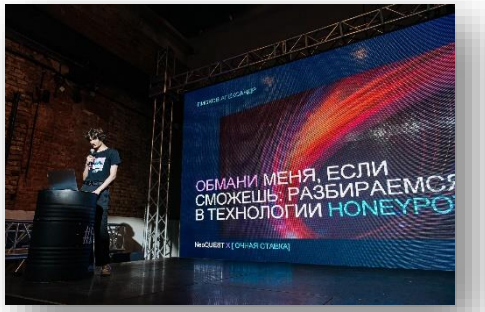
Более 170 экспертных комментариев за 21-22 год

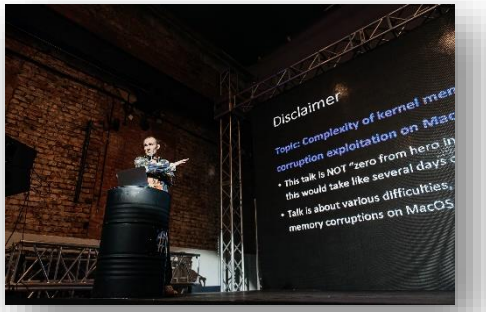
Статьи в популярных журналах, Habr, подкасты, видеоблоги.





NEOQUEST – ЕЖЕГОДНОЕ СОРЕВНОВАНИЕ ПО КИБЕРБЕЗОПАСНОСТИ. ПРОВОДИТСЯ С 2012 ГОДА





- 2000 онлайн и 300 оффлайн участников
- Real-time моделирование кибератак
- Воркшопы и мастер-классы по хакингу и защите
- Конкурсы на взлом и многое другое

Призеры школьного трека NeoQUEST получают + 5 баллов к ЕГЭ !

МОЛОДЕЖНАЯ СЕКЦИЯ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ ИМЕНИ П.Д. ЗЕГЖДЫ «МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ» (МИТСОБИ)

Студенты вузов СПбПУ, ВКА им А.Ф. Можайского, Военная Академия связи, (Санкт-Петербург); МГУ (Москва), МГТУ им. Баумана, МИФИ, Академия ФСО (г. Орел) и др.

Проводится ежегодно

Более 60 докладов

Конкурс докладов

КНИГА ИНСТИТУТА КИБЕРБЕЗОПАСНОСТИ ПО ПОПУЛЯРИЗАЦИИ ПРОФЕССИИ И ПРОФОРИЕНТАЦИИ В IT ДЛЯ СТАРШИХ ШКОЛЬНИКОВ

ВЕБ-ПРИЛОЖЕНИЯ:
АНАЛИЗ БЕЗОПАСНОСТИ

04 | Безопасность мобильных устройств

82

Криптография:
шифр и к шифру

Ярмак
Анастасия Викторовна

научный сотрудник Института кибербезопасности и защиты информации СПбПУ

В случае обычного офлайн-общения достаточно оглянуться по сторонам, чтобы проверить, что никто не подслушивает. Вопреки утверждению о том, что у стен есть уши, среднестатистические стены прослушкой вряд ли занимаются. При общении по сети конфиденциальность переписки обеспечить сложнее. Как гарантировать, что в процессе передачи данные не изменили? Как понять, что собеседник – именно тот, за кого себя выдает? Как доказать другой стороне, что документы принадлежат отправителю? Все из этих вопросов способна решить криптография.

Кратко:

Криптография (с древнегреческого – тайнопись) – это наука о способах преобразования данных с целью их защиты. За длинным словом скрывается понятное желание человека спрятать важную для него информацию от чужих глаз. Речь может идти не только о персональных интересах, но и о военных, государственных, экономических и так далее. Если в детстве вы придумывали собственный язык, то тоже своего рода криптограф.

173

03 | Веб-приложения

Web 1.0, 2.0, 3.0. Создание и эволюция Интернета

Принято считать, что WWW (the World Wide Web) появился в 1990-ых. Именно тогда Тим Бернерс-Ли (Tim Berners-Lee), инженер-программист ЦЕРНа (так называют Европейский центр ядерных исследований, на базе которого построен самый известный в мире ускоритель заряженных частиц – Большой адронный коллайдер), подумал, что современный ему обмен информацией в академических кругах – медленный и ограниченный – сильно тормозит и коммуникацию, и сами разработки. Бернерс-Ли начал искать способы создания более эффективной системы обмена данными.

В марте 1989 года он изложил свое видение того, что должно было стать прототипом Сети, в работе «Управление информацией: предложение». К тому времени уже существовала и функционировала американская сеть

48

04 | Безопасность мобильных устройств

за расходом батареи и сетевой активностью. Если приложение потребляет неадекватно много ресурсов – это повод проверить или даже удалить приложение, так как оно может создавать вредоносную активность.

7. Рекомендуется использовать антивирусные программы от официальных производителей подобных решений.
8. Пользователи обязательно должны использовать многофакторную аутентификацию. Даже двухфакторная аутентификация уже не является надежным средством защиты и может быть легко обойдена злоумышленниками.
9. Рекомендуется периодически создавать резервные копии данных, хранящихся на мобильном устройстве.
10. Пользователи, даже не обладающие техническими знаниями, должны устанавливать настройки, отвечающие за использование шифрования при передаче данных.
11. В дополнение к предыдущему пункту следует упомянуть о запрете на подключение к недоверенным сетям Wi-Fi. Разумеется, под запрет должны попасть публичные сети Wi-Fi.
12. Рекомендуется отключать Wi-Fi и Bluetooth, когда пользователь ими не пользуется.

Конечно, техники атак все время совершенствуются злоумышленниками, но и специалисты по кибербезопасности не дремлют. Правда, они не могут вместо пользователя следить за девайсом, вместо него ограничивать разрешения приложений или менять систему защиты.

Важно помнить, что безопасность личных мобильных устройств во многом зависит от их владельцев. Так что бдительны в первую очередь должны быть именно они.

84

09 | Криптография

История криптографии

На протяжении многих лет единственной задачей, которую решала криптография, было обеспечение секретности передаваемой информации. В древности искусством тайнописи владели единицы, хотя до нас дошли некоторые сведения об очень старых шифрах. Так, например, в Спарте пользовались скиталой – специальным инструментом, с помощью которого греки маскировали свои послания. Узкий цилиндр оборачивался полосой пергамента, на которую наносили текст. Можно спросить: какой же тут секрет? Дело в том, что цилиндры одной ширины и высоты изготавливались по два: один – у отправителя, другой – у получателя. Обернуть пергамент вокруг любой дощечки и прочесть не получалось. Нужен был инструмент именно таких параметров.

Один из самых древних шифров – шифр Цезаря. В наши дни его сможет расшифровать почти кто угодно. Попробуйте. *Ахс тужкоізрлз ретлфгрс ылчусп Щэкгув.* Разгадка простая: буквы сдвигаются дальше по алфавиту на определенное число позиций. В случае с предложением выше – на три. Для расшифровки сообщения, таким образом, достаточно перебрать все возможные комбинации сдвигов и вычислить итог. Естественно, что сейчас для серьезных задач шифр Цезаря уже не используется. Он считается слишком слабым. Его, однако, можно немного усовершенствовать, если сдвигать каждую новую букву на разное количество позиций. Первую, предположим, на две, вторую – на 5, третью – на 7. Этот подход усложнит расшифрование. Последовательность будет определяться ключевой фразой, которую называют гаммой. Гамма, составленная из букв алфавита, с указанием сдвига, служит ключом к шифру. Такой вариант шифрования называют шифром Виженера – в честь французского дипломата Блеза Виженера, убедившего Генриха III использовать шифр. Изъян у этого шифра всё тот же, что у цезаревского – тот, кто правильно подставит первые буквы и верно разгадает гамму, быстро взломает шифр. Для этого не нужен даже компьютер с серьезными мощностями, достаточно немного терпения в простом переборе.

Но не все древние шифры так легко разгадываются. Средневековую рукопись, известную под названием «Манускрипт Войнича», например, так и не

174

расшифровали. Свое название текст получил по имени одного из владельцев. Кто точно его написал – неизвестно. Ровно потому, что неизвестно и содержание. Манускрипт Войнича условно делят на главы по изображениям – «гербарий» (изображены растения), «астрономия» (созвездия), «космология» (круговые диаграммы), «биология» (люди), «фармацевтика» (сосуды). Ученые не могут сойтись даже на едином мнении о языке манускрипта. В 1997 году лингвист Ж. Б. М. Гай предположил, что он написан на двух диалектах одного языка. В 2016 году группа исследователей (А. А. Арутюнов, Л. А. Борисов, Д. А. Зенюк, А. Ю. Ивченко, Е.П. Кирина-Липинская, Ю. Н. Орлов, К. П. Осминин, С. Л. Федоров, С. А. Шилин) выдвинула гипотезу, что текст написан на смешанном языке: 60% – на одном из языков западногерманской группы (английский или немецкий), а 40% текста – на языке романской группы (итальянский или испанский, может быть, латынь). Правда, подтвердить или опровергнуть эти предположения пока нельзя, поскольку манускрипт не расшифрован. Некоторые исследователи считают, что он и не будет расшифрован, потому что вполне может быть мистификацией, бессвязным набором картинок и слов, записанных, чтобы одурачить кого-нибудь.

175

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

ПОЛИТЕХ
Институт кибербезопасности
и защиты информации