Оглавление

[Тексты-оригиналы 1](#_Toc8504375)

[Computer Crime 1](#_Toc8504376)

[Research Centre of Information Technology 1](#_Toc8504377)

[What are the key issues in the IT sector? 3](#_Toc8504378)

[What is ICT? 3](#_Toc8504379)

[Тексты-переводы 4](#_Toc8504380)

[Компьютерное преступление 4](#_Toc8504381)

[Исследовательский Центр Информационных Технологий 4](#_Toc8504382)

[Каковы ключевые проблемы в секторе ИТ? 6](#_Toc8504383)

[Что такое ИКТ? 6](#_Toc8504384)

[Словари терминов 8](#_Toc8504385)

[Computer crime 8](#_Toc8504386)

[Research Centre of Information Technology 8](#_Toc8504387)

[What are the key issues in the IT sector? 9](#_Toc8504388)

[What is ICT? 9](#_Toc8504389)

Тексты-оригиналы

## Computer Crime

Computers can be used to commit all kinds of crimes. It is suggested that one could commit murder by computer if one hacked into an air-traffic controller’s computer system and caused aeroplanes to crash, with the intent to kill the passengers. Not surprisingly crimes that specifically relate to computers are relatively recent creations of statute.

Some specific computer crimes are set out in the Computer Misuse Act 1990. It is designed to protect information kept on computers. There are three particular reasons why such information needs protection by the criminal law. Firstly it is said to be very hard to safeguard information stored on a computer, particularly as often the information is intended to be accessed by a number of authorized people. By contrast information on paper can be kept in a safe or other secure place. Secondly the ease of destroying or corrupting data on a computer means it deserves special protection, particularly as it is not always possible for the owner of the computer to realize that the data have been looked at. Thirdly the highly confidential nature of the kind of information kept on computers (often concerning many members of the public) is such that it needs particular protection.

The act prohibits “hacking”, i.e. gaining unauthorized access to computer material. The offence is committed if a defendant is entering the computer just to see what he can find. The Act also contains a more serious offence of doing this with the intent to commit another offence. The most common example is likely to be a deception offence or theft. A defendant who obtained data which he intended to use in the future to commit an offence of obtaining property by deception will still be guilty of the more serious offence.

There is also an offence of modifying computer material in an unauthorized way. This section is clearly aimed at people who alter computer data with intent to corrupt a program. The intent does not need to be direct towards any particular computer or data. Modification is defined as including removal of any program or data on a computer and includes adding to the contents or erasing them.

It also includes temporary modification. It would appear to cover sending someone a disc with a virus on it that was intended to damage the working of the computer.

It is possible to be guilty of criminal damage of computers if there has been а physical change to some components of the computer.

Research Centre of Information Technology

Research Centre of Information Technology is part of IT4Innovations project, which aims to build a national Centre of Excellence in the field of information technologies. The Centre will enable strengthening concentration of a wide range of scientific disciplines relating to information technologies and thus achieve development in respective spheres. Faculty of Information Technology of Brno University of Technology (FIT BUT) is involved in the project alongside the research leader of this project - VSB - Technical University of Ostrava and other partners - the University of Ostrava, Silesian University in Opava and the Institute of Geonics AS CR.

Part of the project is acquisition of a high-performance supercomputer that is planned to be put into operation in 2014, in which time it is supposed to rank among the top 100 most powerful supercomputers in the world. This supercomputer will be placed in Ostrava.

FIT BUT takes active part in the project as a leader of two work packages Multimedia Information Recognition and Presentation and Secure and Safe Architectures, Networks, and Protocols. The aim of FIT BUT in the project is strengthening the co-operation with the industry.

The **Multimedia Information Recognition and Presentation** research team will systematically investigate the processing of multimedia data, particularly the features on the level of signals acquired by means of various sensors. This will enable multimodal information identification and retrieval as well as research in techniques of efficient computing using multimedia data. The emphasis will especially be put on image, video and speech analysis, document and multimedia data information retrieval, imaging, visualization and modelling including human tissue models, accelerated computing using specialized hardware and techniques of semantic web, formal languages and grammars. The program results in the form of new methods, techniques and knowledge related to the above mentioned fields of research will not only be used to improve the parameters of the existing applications but are also expected to facilitate the creation of completely new applications that have so far been impracticable for both technical and economic reasons.

Main task of the **Secure and Safe Architectures, Networks, and Protocols** research team is systematic development of the concept of security and reliability in the field of information technologies (i.e. development of applications with respect to their security and reliability). Both intentional and accidental abuses of information technologies (IT) represent one of major threats to modern society. In the context of knowledge and IT abuse the demand on the system security becomes as important as its functionality, price or maintainability. Current increase in the complexity of computer systems along with cumulative urgency of tasks they have to cope with requires solving a crucial and highly non-trivial question of how to ensure infallible operation of these systems also in situations in which they are not exposed to potential attacks. Contemporary security and reliability-focused IT research comprises a wide range of issues starting with solving purely mathematical problems (e.g. in the area of cryptographic algorithms or formal verification) up to applied research (e.g. authentication) while making use of the knowledge from a wide range of scientific fields (e.g. biomedicine). Within the research, new methods and approaches are developed and investigated concerning the protection of computer systems against attacks, early detection and identification of the attacker, threat elimination, etc. However, these new methods are also intended for reliable computer systems that make a minimum number of mistakes and are capable of self-configuration and self-healing. Apart from software, the research pays special attention to hardware whose security, reliability and resistance to attacks need to be ensured as well. These concerns e.g. specialized embedded systems and networks providing wireless communication with the surroundings that also need to be secured against both intentional and unintentional abuse.

What are the key issues in the IT sector?

BCS, The Chartered Institute for IT published a report for digital leaders in 2018 which looked at the capabilities, skills and ethics needed in IT organisations in the near-future. It showed that business transformation and organisational change were top priorities and roles in change management, transformation consultancy and business analysis would be on the increase.

The specific skills identified by these organisations included some that would be fully expected - cybersecurity and cloud for example - through to emerging sectors - such as the 'as-a-service' model.

In the survey only 14% of organisations felt they needed bigger budgets - they were in fact looking to educate and train existing staff. That means that graduates, already in the mindset of learning, are well placed to get involved in an industry that is so focused on personal development.

Other areas ripe for careers include agile methodologies, mobile and application development, the internet of things and - increasingly in recent years - artificial intelligence and machine learning. Manipulation of data is a skill that cannot be overlooked, in its many guises - especially that of the relatively new data scientist role - and no doubt we will be hearing about roles in blockchain more and more.

There are other considerations, too, for example the effect that current or incoming legislation have on work - such as GDPR-related roles - that has an implication for big data professionals, who would need skills such things as AWS, Python, Hadoop, Spark, Cloudera, MongoDB, Hive, Tableau, Java and so on.

What is ICT?

**Information Communication Technology (ICT)** is an umbrella term used to encompass all rapidly emerging, evolving and converging computer, software, networking, telecommunications, Internet, programming and information systems technologies. Historically, many of these fields developed separately, in different companies, departments and R&D groups, and at different times. With rapid improvements in computer processing power, networking technology advances, programming interface improvements, widespread adoption of Internet Protocols, integration into organizational strategic operations, and improved workforce and user competencies, however, these fields are rapidly converging.

Once a term used widely outside the United States, ICT is becoming more recognized in the U.S. as this convergence takes place more frequently across the globe, and the demand for professionals who have the knowledge and skills to manage the growing number of intersections is increasing. A degree in ICT is the first step toward a career that will continue to evolve as technology continues to expand the way we create, store, and share data.

ICT students gain knowledge and skills needed to effectively apply, use and manage technology when solving problems specifically related to information and communication. Classes provide a human and organizational focus on technology–teaching students how to be effective users of technology. Students who major in ICT can expect to work in positions where they are the communication link between people, organizations and the technologies used to support those organizations’ information infrastructures.

Тексты-переводы

Компьютерное преступление

Компьютеры могут использоваться для совершения всех видов преступлений. Предполагается, что можно совершить убийство с помощью компьютера, если взломать компьютерную систему авиадиспетчера и вызвать крушение самолета с намерением убить пассажиров. Неудивительно, что преступления, связанные с компьютерами, регулируются относительно недавно созданными законами.

Некоторые компьютерные преступления изложены в законе 1990 года о неправомерном использовании компьютеров. Он предназначен для защиты информации, хранящейся на компьютерах. Существуют три конкретные причины, по которым такая информация нуждается в защите законом. Во-первых, утверждают, что очень трудно защитить информацию, хранящуюся на компьютере, особенно потому, что часто информация предназначена для доступа ряда уполномоченных лиц. Напротив, информацию на бумаге можно хранить в сейфе или другом надежном месте. Во-вторых, легкость уничтожения или порчи данных на компьютере означает, что они заслуживает особой защиты, особенно, поскольку владелец компьютера не всегда может понять, что данные были просмотрены. В-третьих, крайне конфиденциальный характер информации, хранящейся на компьютерах (часто касающейся многих представителей общественности), таков, что она нуждается в особой защите.

Закон запрещает "взлом", т. е. получение несанкционированного доступа к компьютерным материалам. Преступление считается совершённым, если подсудимый входит в компьютер, чтобы что-то там найти. В законе также имеется информация о более серьезном преступлении, заключающимся в совершении этого деяния с намерением совершить другое преступление. Наиболее распространенным примером преступления, является обман или кража. Обвиняемый, получивший данные, которые он намеревался использовать в будущем для совершения преступления, связанного с получением имущества путем обмана, будет по-прежнему виновен в более серьезном преступлении.

Существует также правонарушение: «Незаконное изменение компьютерных материалов». Этот раздел явно предназначен для людей, которые изменяют компьютерные данные с намерением испортить программу. Намерение может быть не направлено непосредственно на какой-либо конкретный компьютер или данные. Модификация – это удаление какой-либо программы или данных на компьютере или добавление к содержимому, удаление из него.

Это правонарушение также включает временные изменения. Оно касается и отправки кому-то диска с вирусом, который должен был повредить работу компьютера.

Можно быть виновным в причинении ущерба компьютерам, если произошли физические изменения некоторых компонентов компьютера.

Исследовательский Центр Информационных Технологий

Исследовательский Центр Информационных Технологий является частью проекта IT4Innovations, который нацелен на создание национального Центра Превосходства в области информационных технологий. Центр позволит укрепить концентрацию широкого спектра научных дисциплин, относящихся к информационным технологиям и, таким образом, достичь развития в соответствующих областях. Факультет Информационных Технологий Брненского Университета Технологий (FIT BUT) участвует в проекте вместе с исследовательским руководителем этого проекта – VSB – Технический Университет Остравы и другие партнеры – Университет Остравы, Силезийский Университет в Опаве и Институт Геоники AS CR.

Частью проекта является приобретение высокопроизводительного суперкомпьютера, который планируется ввести в действие в 2014, в то время, когда он должен войти в топ 100 самых мощных суперкомпьютеров в мире. Этот компьютер будет размещен в Остраве.

FIT BUT принимает активное участие в проекте в качестве главы двух рабочих пакетов: «Распознавание и Представление Мультимедийной Информации» и «Безопасность и Безопасные Архитектуры, Сети и Протоколы». Целью FIT BUT в проекте является укрепление сотрудничества с промышленностью.

Исследовательская группа по «Распознаванию и Представлению Мультимедийной Информации» будет систематически исследовать обработку мультимедийной информации, в частности особенности на уровне сигналов, получаемых с помощью различных датчиков. Это сделает возможным идентификацию и поиск мультимодальной информации, а также исследование методов эффективного вычисления с использованием мультимедийных данных. Особое внимание будет уделено анализу изображений, видео и речи, поиску информации о документах и мультимедийных данных, обработке изображений, визуализации и моделированию, включая модели ткани человека, ускоренные вычисления с использованием специализированного аппаратного обеспечения и методов семантической сети, формальных языков и грамматик. Результаты программы в форме новых методов, приемов и знаний, относящихся к вышеупомянутым областям исследования, будут использованы не только для улучшения параметров существующих применений, но также ожидается, что они будут способствовать созданию совершенно новых применений, которые до сих пор были невыполнимы по техническим и экономическим причинам.

Главной задачей исследовательской группы «Безопасность и Безопасные Архитектуры, Сети и Протоколы» является систематическая разработка концепции безопасности и надежности в области информационных технологий (т.е. разработка приложений с точки зрения их безопасности и надежности). Как преднамеренные, так и случайные злоупотребления информационными технологиями (ИТ) представляют собой одну из основных угроз для современного общества. В контексте знаний и злоупотреблений в сфере ИТ, потребность в безопасности системы становится такой же важной, как ее функциональность, цена или стабильность. Текущее увеличение сложности компьютерных систем наряду с совокупной срочностью задач, с которыми им приходится сталкиваться, требует решения крайне важного и довольно нетривиального вопроса о том, как обеспечить безошибочную работу этих систем также в ситуациях, когда они не подвергаются потенциальным атакам. Современные ИТ-исследования, ориентированные на безопасность и надежность, включают в себя широкий круг проблем, начиная с решения чисто математических задач (например, в области криптографических алгоритмов или формальной проверки) до прикладных исследований (например, аутентификации), при этом используя знания из широкого спектра научных областей (например, биомедицина). В рамках исследования разрабатываются и исследуются новые методы и подходы, касающиеся защиты компьютерных систем от атак, раннего обнаружения и идентификации злоумышленника, устранения угроз и т. д. Однако эти новые методы также предназначены для надежных компьютерных систем, которые делают минимум количество ошибок и способны к самоконфигурации и самовосстановлению. Помимо программного обеспечения, исследование уделяет особое внимание аппаратному обеспечению, безопасность, надежность и устойчивость к атакам которого, также должны быть обеспечены. Это касается, например, специализированных встроенных систем и сетей, обеспечивающих беспроводную связь с окружающей средой, также должны быть защищены от преднамеренного и непреднамеренного злоупотребления.

Каковы ключевые проблемы в секторе ИТ?

БКО, Аккредитованный ИТ Институт опубликовал отчет для цифровых лидеров в 2018 году, в котором рассматривались возможности, навыки и этика, необходимые ИТ-организациям в ближайшем будущем. Он показал, что трансформация бизнеса и организационные изменения были главными приоритетами, и должности в управлении изменениями, консультации по трансформации и бизнес-анализе будут более значимыми.

Специфические навыки, определенные этими организациями, включали в себя те, которые будут вполне ожидаемы - например, кибербезопасность и облако, благодаря новым секторам - например, модель «как услуга».

В ходе опроса только 14% организаций отметили, что им требовались более большие бюджеты - они на самом деле хотели обучить и натренировать существующий персонал. Это означает, что выпускники, настроенные на обучение, имеют хорошие возможности для участия в индустрии, которая так сосредоточена на личностном развитии.

К другим областям, готовым для карьеры, относятся гибкие методологии, мобильная разработка и разработка приложений, интернет вещей и - растущие в последние годы - искусственный интеллект и машинное обучение. Манипулирование данными – это навык, который нельзя игнорировать, во многих его проявлениях, особенно относительно новой роли специалиста по анализу данных, и, без сомнения, мы будем все больше и больше слышать о ролях в блокчейне.

Есть и другие соображения тоже, например, влияние, которое оказывает действующее или поступающее законодательство на работу, например, на роли, связанные с ОРЗД, которые имеют значение для профессионалов, работающих с большими объемами данных, которым потребуются такие навыки, как AWS, Python, Hadoop, Spark, Cloudera, MongoDB, Hive, Tableau, Java и так далее.

Что такое ИКТ?

Информационно-коммуникационные технологии (ИКТ) - это общий термин, который охватывает все быстро развивающиеся, эволюционирующие и объединяющиеся технологии компьютеров, программного обеспечения, сетей, телекоммуникаций, интернета, программирования и информационных систем. Исторически многие из этих областей развивались отдельно, в разных компаниях, отделах и группах исследования и разработки, и в разное время. В условиях быстрого улучшения вычислительной мощности компьютеров, прогресса сетевых технологий, улучшения интерфейса программирования, широкого внедрения интернет-протоколов, интеграции в организационные стратегические операции и повышения квалификации персонала и компетенции пользователей, однако эти области быстро сходятся.  
  
Когда термин начинает широко использоваться за пределами Соединенных Штатов, ИКТ становится все более узнаваемым в США, поскольку эта конвергенция происходит чаще по всему миру, и спрос на профессионалов, обладающих знаниями и навыками для управления растущим числом пересечений, растет. Научная степень в области ИКТ является первым шагом к карьере, которая будет продолжать требоваться по мере того, как технологии продолжают расширять способы создания, хранения и обмена данными.  
  
ИКТ-студенты приобретают знания и навыки, необходимые для эффективного применения, использования и управления технологиями при решении проблем, особенно связанных с информацией и коммуникацией. Специальности обеспечивают человеческий и организационный акцент на технологии - обучение студентов тому, как быть эффективными пользователями технологии. Студенты, специализирующиеся на ИКТ, могут рассчитывать на работу на должностях, где они являются связующим звеном между людьми, организациями и технологиями, используемыми для поддержки информационной инфраструктуры этих организаций.

# Словари терминов

## Computer crime

1. ease (n) – легкость, простота
2. gain (v) – получать
3. offence (n) – преступление
4. defendant (n) – подсудимый, обвиняемый
5. deception (n) – обман
6. obtain (v) – получать
7. guilty (adj) – виновный
8. corrupt (v) – портить

Research Centre of Information Technology

1. aim (v) – быть нацеленным
2. field (n) – поле, область
3. excellence (n) – превосходство
4. enable (v) – позволять, делать возможным
5. relate to (v) – относиться к
6. respective (adj) – соответствующий
7. acquisition (n) – приобретение
8. to put into operation (v) – вводить в действие
9. strengthening (v) – укреплять
10. investigate (v) – исследовать
11. acquire (v) – получать
12. emphasis (n) – внимание
13. tissue (n) – ткань
14. semantic (adj) – семантический
15. threat (n) – угроза
16. cumulative (adj) – совокупный
17. urgency (n) – срочность
18. infallible (adj) – безошибочный
19. contemporary (adj) – современный
20. comprise (v) – содержать, включать
21. concern (v) – касаться
22. reliability (n) – надежность
23. intentional (adj) – намеренный
24. abuse (n) – злоупотребление
25. maintainability (n) – ремонтопригодность
26. cope (v) – справляться
27. expose (v) – подвергать
28. elimination (n) – устранение
29. embed (v) – встраивать
30. surroundings (n) - окружение

What are the key issues in the IT sector?

1. chartered (adj) – привилегированный
2. ripe (adj) – готовый
3. agile (adj) – гибкий
4. guise (n) – облик, проявление
5. legislation (n) – законодательство
6. mindset (n) – познание
7. emerge (v) – зарождаться
8. capability (n) – возможность
9. consultancy (n) – консультирование
10. survey (n) – исследование
11. implication (n) – импликация, причастность
12. expect (v) – ожидать
13. graduate (n) – выпускник
14. doubt (n) – сомнение
15. consideration (n) – рассмотрение

What is ICT?

1. encompass (v) – охватывать
2. converge (v) – сходиться, объединять
3. emerging (adj) – возникающий
4. rapid (adj) – быстрый
5. improvement (n) – улучшение
6. widespread (adj) – широкий, распространенный
7. adoption (n) – принятие
8. integration (n) – интеграция, объединение
9. demand (n) – потребность
10. major (adj) – основной, профильный
11. separate (adj) – отдельный
12. advance (n) – продвижение, прогресс
13. recognize (v) – узнать
14. expand (v) – расширять
15. link (n) – связь