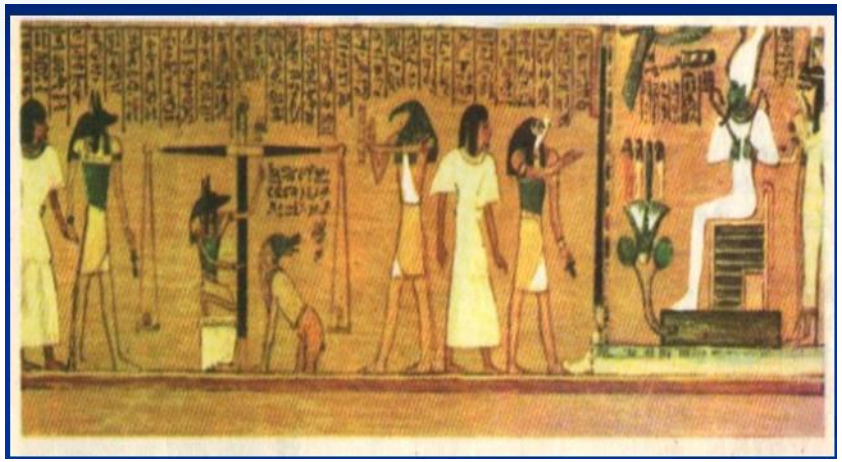
Необходимость компьютерной криминалистики (forensics)как науки

Урденко О.Г.

История развития криминалистики

- **Около 1300 г. до н. э.**
- Самое древнее из сохранившихся до нашего времени уголовных дел: протоколы расследования ограблений гробниц в Древнем Египте



История развития криминалистики

- **Около 250 г. до н. э.**
- — Древнегреческий врач Эрасистрат заметил повышение частоты пульса у человека, говорящего неправду, — позже это станет критерием, который оценивает «детектор лжи»
- — Архимед измерил плотность сплава и выявил факт хищения золота ювелиром, которому была заказана корона тирана Сиракуз

История развития криминалистики

- **1008 г. н. э. Афганский султан Махмуд Газневи объявил в розыск врача Авиценну** и велел развесить его портреты на воротах всех городов страны. Древнейшая известная нам попытка использовать изображение при розыске человека

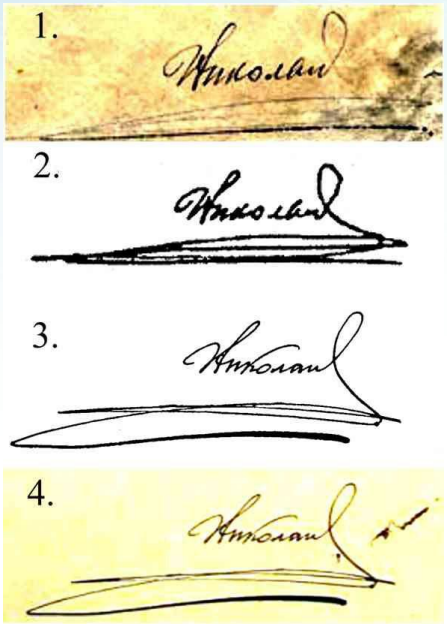
История развития криминалистики

- **1248 г. В Китае вышло руководство для следователей** с описанием методики установления факта насильственной смерти от удушения или утопления

- 1302 г. В Болонье (Италия) врач Бартоломео да Вариньяна произвел первое в Европе вскрытие в интересах суда

История развития криминалистики

1595 г. В Париже присяжные письмоведы приступили к графологической экспертизе документов, фигурирующих в уголовных делах



История развития криминалистики

- **1712 г. Петр I** при посещении дома-музея Мартина Лютера осмотрел чернильное пятно в том месте стены, куда Лютер метнул чернильницу, целясь в явившегося ему дьявола. Заключение Петра: «Чернила новые, и все сие неправда»

История развития криминалистики

- **1838 г. Во Франкфурте вышло первое руководство по сбору вещественных доказательств и криминалистической тактике**. На этой работе Людвига фон Ягеманна основаны современные методики осмотра места происшествия и работы с подследственными
- **1840 г. Матье Орфила** впервые изобличил отравителя по данным химического анализа содержимого желудка отравленного

История развития криминалистики

- **1883 г. В Париже Альфонс Бертильон** с помощью данных антропометрии изобличил преступника, назвавшегося чужим именем: впервые личность установлена с помощью точных измерений

История развития криминалистики

- **1891 г. В Буэнос-Айресе** полицейский Хуан Вучетич впервые изобличил преступника по отпечаткам пальцев и начал дактилоскопировать задержанных

История развития криминалистики

- 1897 г. Австрийский ученый Ганс Гросс назвал науку о раскрытии преступлений «криминалистика»

История развития криминалистики

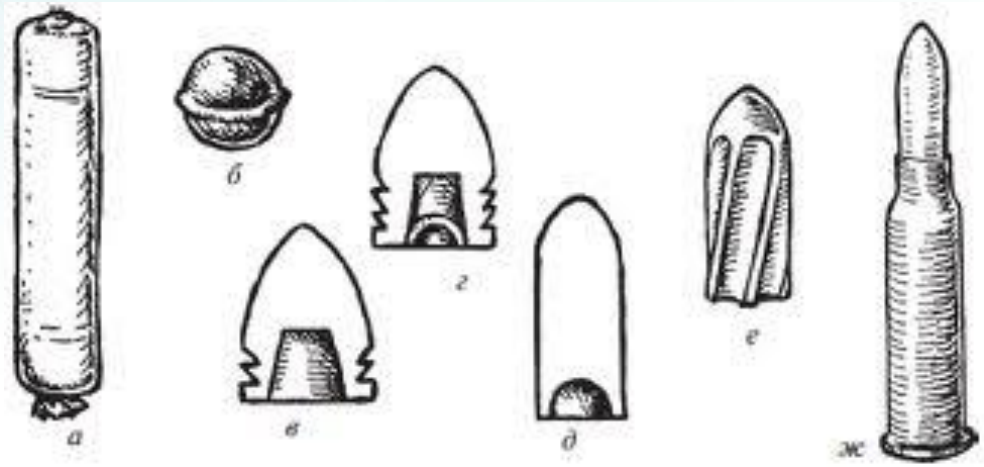
- 1910 г. В Лионе Эдмон Локар создал первую полицейскую криминалистическую лабораторию

История развития криминалистики

- **1917 г. Первый удачный опыт применения детектора лжи**. Судмедэксперт Вильям Марстон из Гарварда сделал аппарат, замерявший систолическое давление крови у испытуемого, когда ему задают разные вопросы. Исследование сузило круг подозреваемых из 70 лиц, имевших доступ к документам, копии которых попадали в германское посольство. Слежка позволила поймать одного из них на встрече с немецким агентом

История развития криминалистики

- **1920 г. Группа нью-йоркских криминалистов выработала надежные методы идентификации огнестрельного оружия**, из которого выпущена исследуемая пуля



История развития криминалистики

- **1970 г. Первые преступления, обнаруженные из космоса**. Экипаж околоземной станции «Союз-9» проводил измерения площади сельхозугодий в Европейской части СССР. Оказалось, что руководители колхозов и совхозов указывали в документах неверные сведения. На юге распахивали и засевали на 30% больше земель, чем на бумаге, и завышали урожайность. На севере, напротив, настоящие поля были намного меньше, чем по документам

Компьютерная криминалистика и сбор доказательств

Расследования

Компьютерная криминалистика и сбор доказательств

- Число компьютерных преступлений постоянно растет, поэтому специалистам по безопасности важно понимать, как должно проводиться расследование таких преступлений.

Компьютерная криминалистика и сбор доказательств

- Это включает в себя понимание требований законодательства к конкретным ситуациям, системы охраны вещественных доказательств, понимание того, какие доказательства приемлемы для использования в суде, какие следует применять процедуры реагирования на инциденты.

Правовые процедуры

- При расследовании компьютерного преступления важно правильно выполнить все необходимые для этого процедуры, предусмотренные законодательством.

Правовые процедуры

- Это необходимо, чтобы собранные доказательства могли быть приняты в суде и при необходимости были проверены. Любое нарушение процедуры сбора доказательств может привести к тому, что доказательства не будут приняты судом и это разрушит все дело.

Специалист по безопасности

- должен понимать, что расследование касается не только потенциальных улик на жестком диске – оно будет проводиться в отношении всего окружения: люди, сеть, любые подключенные внутренние и внешние системы.

Реагирование на инциденты

- **Событие** – это отрицательное происшествие, которое можно выявить, проверить и задокументировать.
- **Инцидент** – это последовательность событий, которые отрицательно влияют на компанию и/или воздействует на состояние ее безопасности.

Реагирование на инциденты

- поэтому называется реагирование на подобные проблемы «реагированием на инциденты» и «обработкой инцидентов», именно инциденты вызывают нарушения безопасности и ведут к негативному влиянию на компанию.

Виды инцидентов

- вирусы
- инсайдерские атаки
- хакерские атаки
- взлом входа в сеть
- мошенничество в банковской системе
- утечки или повреждения информации
- и т.п.

Подходы расследований

- Компьютерные преступления могут иметь правовые последствия, которые не сразу заметны и к которым нужно подходить с осторожностью.

Подходы расследований

- Во всех случаях работы специалиста по расследованию инцидента с доказательствами, представленными в цифровой или электронной форме, при хранении или передаче электронных данных применяется компьютерная криминалистика

Компьютерная криминалистика (forensics)

- **Форе́нзика -** прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств. (Федотов Н.Н.)

- На бытовом уровне криминалистика понимается как наука про раскрытие преступлений.
- В прошлом во многих странах западной Европы этим термином пользовались для определения всей совокупности криминалистических наук.

История компьютерной экспертизы

- **В сентябре 1976 года**, в сенат США был внесен проект закона про использование компьютерных программ и сохранения на носителях программного кода, а также фиксирования производителем программ, данных про разработчика.

История компьютерной экспертизы

- **В 1977 году** был принят закон про несанкционированное использование компьютерных программ. Что послужило началу проведения экспертиз связанных с компьютерными программами.

- **Компьютерная криминалистика является достаточно новым направлением криминалистики**. Из-за этого, а также из-за ее сложности, у многих компаний недостаточно навыков в этой области.

Компьютерная криминалистика

- Компьютерная криминалистика не относится непосредственно к компьютерному оборудованию или программному обеспечению.

Компьютерная криминалистика

- Это набор специальных процедур, предназначенных для реконструкции процесса работы на компьютере, анализа остаточных данных, проведения проверки подлинности данных с помощью средств технического анализа, исследования технических свойств данных.

Квалификация специалиста

- Люди, которые проводят компьютерные расследования, должны иметь необходимую квалификацию в этой области, **они должны точно знать, как и что нужно искать**.

Международные организации по компьютерным доказательствам

- При работе с цифровыми доказательствами должен применяться единообразный подход, чтобы они могли использоваться в различных судах разных стран.

Международные организации по компьютерным доказательствам

- ***IOCE*** (International Organization on Computer Evidence) – Международная организация по компьютерным доказательствам
- В США организация ***SWDGE*** (Scientific Working Group on Digital Evidence) – Научная рабочая группа по цифровым доказательствам

Международные организации по компьютерным доказательствам

- целью IOCE и SWDGE является обеспечение единообразного подхода для всего сообщества экспертов по компьютерной криминалистике.

Принципы IOCE / SWDGE

- При работе с цифровыми доказательствами должны быть применимы все основные процессуальные принципы и принципы компьютерной криминалистики.

Принципы IOCE / SWDGE

- Действия, выполняемые в процессе сбора цифровых доказательств, не должны изменять эти доказательства.

Принципы IOCE / SWDGE

- Допуск к оригинальным цифровым доказательствам может быть предоставлен при необходимости только лицу, прошедшему специальное обучение по работе с ними.

Принципы IOCE / SWDGE

- Все действия, связанные со сбором, использованием, хранением или передачей цифровых доказательств, должны быть надлежащим образом задокументированы, а документы должны быть сохранены и доступны для изучения.

Принципы IOCE / SWDGE

- Лицо несет ответственность за все действия в отношении цифровых доказательств, которые находятся в его распоряжении.

Принципы IOCE / SWDGE

- Любое учреждение, в обязанности которого входит сбор, использование, хранение или передача цифровых доказательств, несет ответственность за соблюдение этих принципов.

Специалисты по расследованию инцидентов

- Специалисты по расследованию инцидентов (incident investigator, следователь) – это люди с специальными знаними.

Специалисты по расследованию инцидентов

- Специалист по расследованию инцидентов - разбираться в процедурах компьютерной экспертизы, сбора доказательств, знает, как проводить анализ ситуации, чтобы понять произошедшее, уметь найти важные улики в системных журналах.

Криминалистические принципы проведение сбора доказательств

- - определение места преступления,
- - защита окружения от изменений и утраты улик,
- - нахождение улик и потенциальных источников улик,
- - сбор улик.

Доказательство

- Любое доказательство имеет свой жизненный цикл

Жизненный цикл доказательства включает в себя:

- Выявление и сбор
- Обеспечение сохранности и транспортировка
- Предъявление в суде
- Возврат доказательства жертве или владельцу

- Чтобы преступление было успешно раскрыто, а преступник понес адекватное наказание, необходимы надежные доказательства. Без правильного проведения компьютерных исследований и экспертизы, вероятность успешного предъявления доказательств компьютерного преступления в суде значительно снижается

- Вопросы законодательства и проведения расследований являются очень важной частью компьютерной и информационной безопасности. К сожалению, компании редко о них задумываются, пока они не сталкиваются с компьютерными преступлениями. Эти вопросы необходимо рассматривать, если мы всерьез хотим бороться с компьютерной преступностью и добиваться адекватного наказания компьютерных преступников.

- Спасибо за внимание

Лаборатория компьютерной криминалистики и информационной безопасности

Эксперт Урденко А.Г.

- ekspertlkd@ukr.net