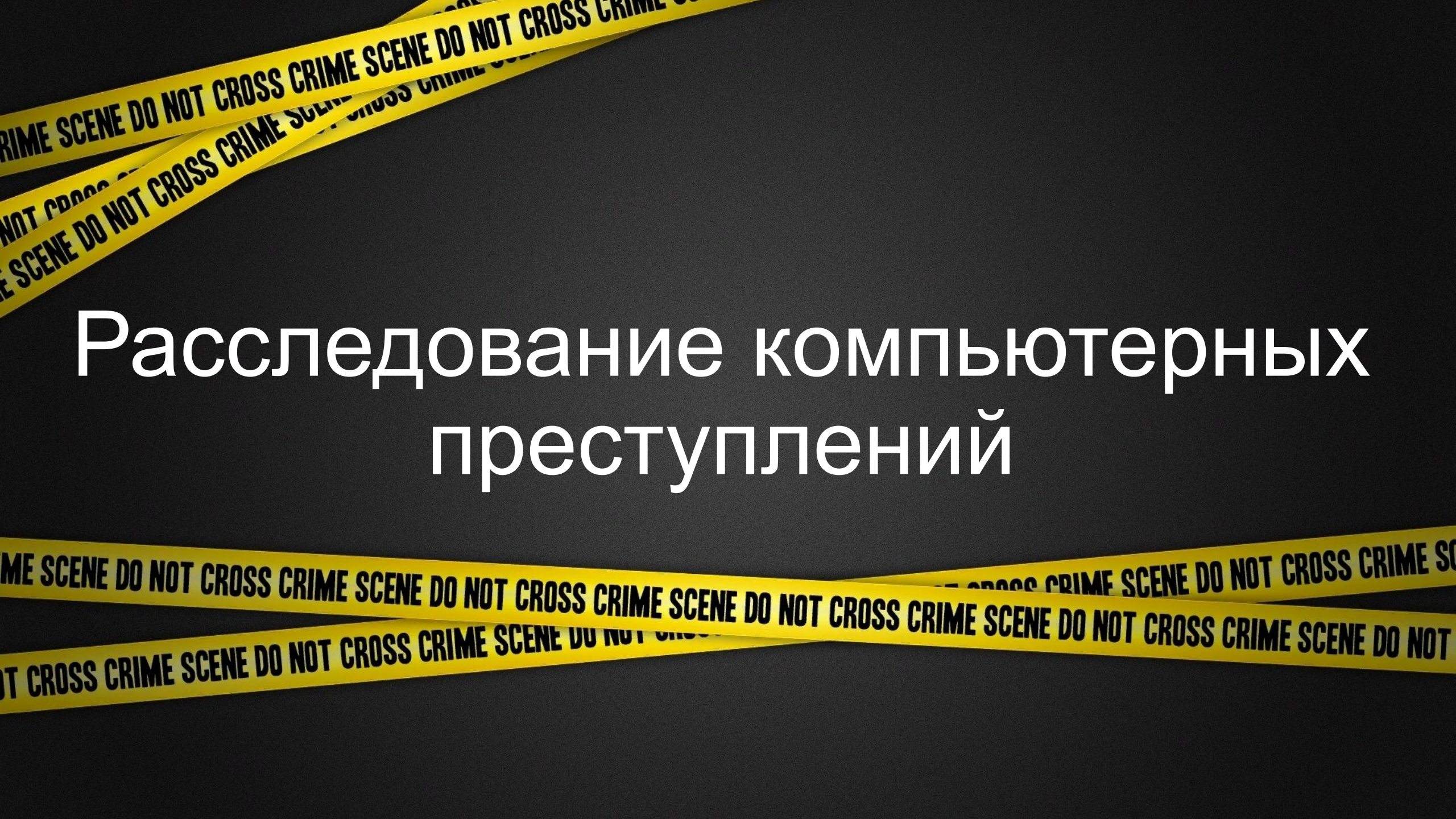


Расследование компьютерных преступлений

Развитие современного общества, основанного на использовании огромного количества самой разнообразной информации, немыслимо без широкого внедрения во все сферы жизни общества электронно-вычислительной техники. Она служит не только для хранения и обработки соответствующей информации на уровне отдельных управленческих или хозяйственных единиц или использования как средства связи между гражданами, но и широко внедряется в целях обеспечения внутренней и внешней безопасности различных государств.
Но, как всем известно, человек найдет способы использовать абсолютно любое благо или достижение в своих целях.

Именно поэтому и появились компьютерные преступления.

Компьютерная преступность (преступление с использованием компьютера) — представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Стр
компьютерной
преступности в разных странах
существенно отличается друг от
друга. В юридическом понятии,
компьютерных преступлений, ка
преступлений специфических н
существует.

С развитием информацизации бизнеса многократно увеличивается уровень возможных финансовых потерь, что увеличивает интерес киберпреступников к противозаконному заработку.

С каждым годом частота преступлений в компьютерной сфере и объем наносимого ущерба увеличивается в геометрической прогрессии.

Основная тому причина – высокая доходность такого противозаконного бизнеса и лазеек в законодательной и судовой практике различных стран.

Виды компьютерных преступлений

В зависимости от способа воздействия на компьютерную систему специалисты выделяют четыре вида компьютерных преступлений:

- Физические злоупотребления, которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.
- Операционные злоупотребления, представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств.
- Программные злоупотребления, которые включают в себя: различные способы изменения системы математического обеспечения («логическая бомба» – введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; «троянский конь» – включение в обычную программу своего задания).
- Электронные злоупотребления, которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

Особенности методики расследования преступлений

Замечание: методика расследования компьютерных преступлений, а именно криминалистическая характеристика таких деяний, формируется при учете их высокой латентности, степени сложности сбора доказательств, включая их использование в процессе доказывания.

Методика расследования преступлений в сфере компьютерной информации включает:

- информацию о способах совершения и сокрытия преступных деяний;
- типологические данные, касающиеся субъектов преступления;
- информация об обстановке и типичном мотиве совершения преступления.

Большую роль играет знание о личности преступника, поскольку это несет в себе важную для криминалистики информацию. Так, в уголовном расследовании, особенно важными являются сведения о профессиональных качествах, специальных знаниях, навыках работы с ЭВМ, программами компьютера и др.

Субъекты классифицируются на несколько групп: профессионалы в области взлома компьютерных программ и сетей (вандалы), которые занимаются распространением вредоносных программ (вирусов) для разрушения системы.

Другие субъекты вносят в компьютерную систему звуковые, шумовые эффекты (шутники), еще одна группа взламывает компьютерную систему для похищения денежных средств (взломщики).

Не профессиональные преступники в сфере компьютерных технологий могут заниматься блокировкой, игнорированием информации, что чаще всего происходит в компьютере без пароля или с паролем, который знает определенных круг людей. В эту категорию можно включить и лиц, которые имеют различные психические отклонения и страдают компьютерными

Расследование преступлений

Расследование преступлений в сфере компьютерной информации показало, что подобные преступления чаще совершаются мужчинами 16-30 лет. В их числе преобладают те, кто имеет высшее и неоконченное высшее образование.

В соответствии с обстановкой совершения компьютерных преступлений значительную роль играет место и время совершения. Для этих действий не всегда место совершения проти деяния совпадает с местом наступления опасных последствий для общества. В большинстве случаев преступле условиях нарушения установленного порядк компьютера. Время в этом случае устанавливается по датам, которые указаны файлах.

Замечание: среди мотивов преступления можно выделить шпионаж и диверсию, корысть, хулиганство и др.

На начальной стадии расследования такого преступления обычно проявляются следующие виды типовых ситуаций:

- заявление о неправомерном доступе к чужим сведениям (нарушение целостности и конфиденциальности информации), поступающее от собственника информационной системы, который обнаруживает этот факт; наличие информации о лице, которое может иметь к этому отношение;
- заявление пострадавшего лица при отсутствии информации о причастности к противоправным деяниям определенного лица;
- обнаружение факта указанных противоправных действий оперативными органами в ходе розыска, включая их фиксацию соответствующим образом.

Во всех случаях основная первоначальная задача должна сводиться к установке способа совершения преступления; порядка регламентации определенной информационной системы посредством ее собственника; людей, которые работают с системой и имеют к ней доступ.

Для этого осуществляются первоначальные следственные действия, включая допрос собственника информационной системы и свидетелей; осмотр компьютера (техники) и носителей; выемка и осмотр необходимых документы. Осмотр и выемка проводятся при участии специалистов в сфере компьютерной техники, при этом участие специалистов в сфере компьютерной информации может являться специфической методической особенностью таких расследований.

Рассмотренные действия позволяют осуществить выявление и других необходимых свидетелей для допроса, определение людей, которые причастны к этому деянию, расчет примерной суммы ущерба, который причинен владельцу информационной системы.

Замечание: в случае задержания правонарушителя на месте преступления (сразу после него), необходим его обыск и допрос. Обыск производится у него дома и на работе.

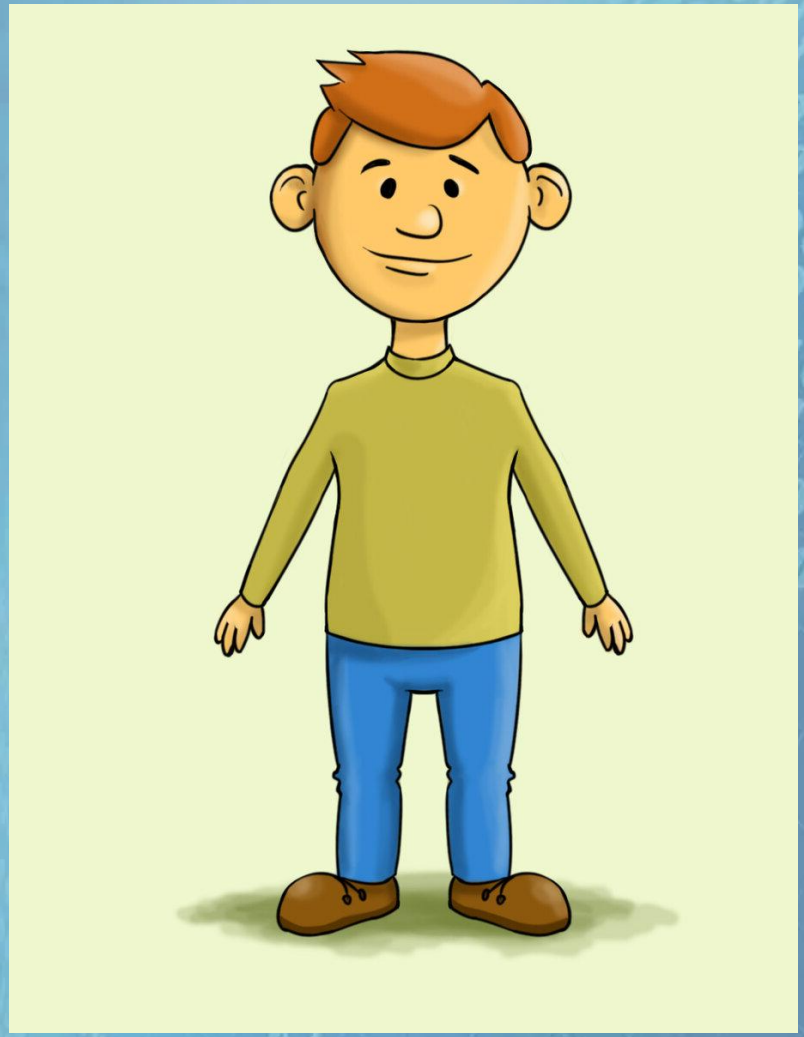
Последующие следственные действия касаются изъятия компьютера, его устройств, их осмотра и при необходимости экспертного исследования, допроса новых свидетелей, предъявления обвинения и допроса обвиняемого.

Комплекс мероприятий по расследованию компьютерных преступлений

1) Восстановление хронометража событий
2) Выявление причин произошедшего инцидента информационной безопасности
3) Выявление возможных виновников инцидента
4) Анализ уязвимостей внедренного в организации режиме обеспечения безопасности коммерческой тайны, выработка мер по их устранению
5) Оформление информации в качестве юридически значимой доказательной базы

Кто может стать жертвой?

Как ни странно, но абсолютно любой. Будь то обычный человек, будь то крупный бизнесмен, будь то целая компания.



Несколько впечатляющих хакерских атак

В июне 2010 года исследования в сфере компьютерной безопасности открыли компьютерный вирус Stuxnet, предназначенный для атаки программируемых логических контроллеров, применяющихся в промышленном оборудовании.

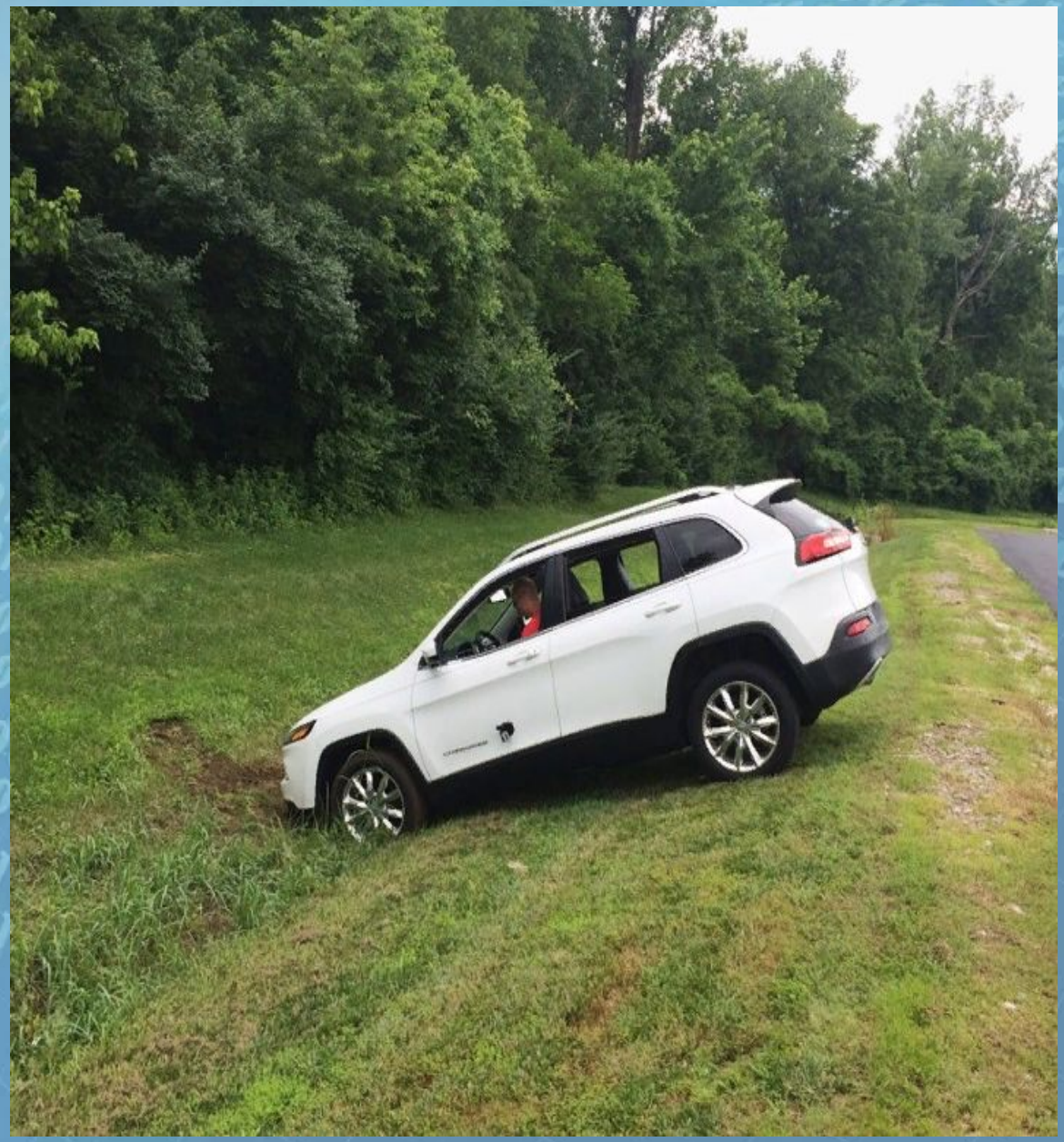
Предполагается, что вирус был создан американо-израильской командой для атаки иранского завода по обогащению урана в Натанзе. Вирус предназначен для изменения скорости центрифуг по обогащению урана путем генерирования колебаний, достаточно сильных для уничтожения устройств. Согласно отчетам, с помощью Stuxnet уже повреждены более 1000 центрифуг, таким образом, сократив количество эксплуатируемых в Иране устройств до 3900.

Взломанный «джип»

Энди Гринберг вел свой Jeep Cherokee со скоростью около 110 км/ч, когда с машиной начало твориться что-то неладное. Система кондиционирования вдруг начала дуть холодным воздухом на полную мощность, радио само переключилось и заиграло хип-хоп, дворники стали что есть силы елозить по стеклу, а из форсунок на капоте полились потоки «омывайки». Ну а затем на дисплее мультимедийной системы появилось изображение двух хакеров, которых Энди хорошо знал, – Чарли Миллера и Криса Валашека. Эта парочка взломала «джип» Гринберга.

Нет, хакеры не точили зуб на журналиста Wired, пишущего про информационную безопасность. Просто Миллер и Валашек смогли взломать «Чероки» так, что им можно было удаленно управлять через Интернет, – и по совместной договоренности демонстрировали это Гринбергу максимально наглядно. Удаленно управлять – значит не только менять музыку, но еще и отключать тормоза, поворачивать руль и нажимать на газ: все это Энди тоже успел испытать на собственной шкуре, когда его автомобиль вдруг сам повернул руль и съехал в кювет, правда, предварительно замедлившись. Пожелай хакеры угробить журналиста – они могли бы без проблем реализовать и это, но такой договоренности с Гринбергом у них определенно не было.

Взлом «джипа» в 2015-м – первая атака на автомобиль, показавшая, насколько серьезными могут быть последствия. Именно после того, как Гринберг опубликовал свою статью, а Миллер и Валашек выступили с докладом о взломе на нескольких конференциях, автопроизводители наконец-то начали думать о безопасности автомобилей не только в контексте подушек, шторок, жесткости кокпита и наличия систем экстренного торможения, а еще и с точки зрения защиты от кибератак. После этой демонстрации и многие другие хакеры решили попробовать свои силы во взломе автомобилей – и нашли еще множество уязвимостей. Особым вниманием, конечно же, пользовалась «Тесла», которую за последние три года неоднократно взламывали команды из разных стран, заставляя ее ездить без водителя, открывать двери, резко тормозить и так далее.



Заключение

Оценивая современное состояние уголовной и криминалистической теории следует признать, что в целом проблемы уголовно-правовой характеристики, совершенствования практики раскрытия, расследования и предупреждения компьютерных преступлений изучены явно неточно.

Необходимость всестороннего исследования обозначенных проблем диктуется как потребность следственной практики, так и задачами дальнейшего совершенствования как уголовно-правовой, так и криминалистической теории, усиления их влияния на результаттивность борьбы с компьютерной преступностью.