

**ОБЯЗАННОСТЬ ЮРИСТА В ОБЛАСТИ
ТЕХНОЛОГИЙ –**

**ЧТО ДОЛЖЕН ЮРИСТ, СОБЛЮДАЮЩИЙ
ПРОФЕССИОНАЛЬНУЮ ЭТИКУ, ЗНАТЬ О
ТЕХНОЛОГИИ?**

Ана Хурцидзе

Тбилиси, Грузия

2020

АМЕРИКАНСКАЯ АССОЦИАЦИЯ ЮРИСТОВ -
ТИПОВЫЕ ПРАВИЛА ПРОФЕССИОНАЛЬНОЙ
ОТВЕТСТВЕННОСТИ

Комментарий 8 к Правилу 1.1,

Юристы должны “быть в курсе изменений в законе и его практике, в том числе знать о преимуществах и рисках, связанных с соответствующими технологиями.”

В настоящее время тридцать один штат принял правила, требующие технологической компетентности.

КАКИЕ ТИПЫ ТЕХНОЛОГИЙ ИСПОЛЬЗУЮТ ЮРИСТЫ?

- **Локальные технологии** - основные компьютеры, домашние компьютеры, операционные системы, серверы юридических фирм, мобильные устройства, такие как ноутбуки, смартфоны и планшеты, принтеры, сканеры, копиры, внешние жесткие диски, внешние носители и электронная почта.
- **Облачные технологии** - технологии, контролируемые третьими сторонами и доступные через Интернет.

ЧТО ДОЛЖЕН ЗНАТЬ ЮРИСТ, СОБЛЮДАЮЩИЙ ПРОФЕССИОНАЛЬНУЮ ЭТИКУ, О ТЕХНОЛОГИЯХ?

- Понимать риски кибербезопасности и угрозы подключения к Интернету и соответственно защищать и обезопасить информацию о клиентах;
- Использовать Интернет в соответствии с этической ответственностью для развития клиентов через веб-сайты, социальные медиа и маркетинг;
- Предоставлять более эффективные юридические услуги с использованием облачных систем для управления юридической практикой;
- Проводить предоставление электронных данных/доказательств в судебные процессы, иногда приобщая большие объемы информации, которая требует привлечения сторонних лиц к расследованию, услугам по сбору данных и документообороту.

КАКИЕ ТЕХНОЛОГИЧЕСКИЕ НАВЫКИ ИМЕЮТСЯ?

1. **Нормы кибербезопасности** = Разумные меры безопасности для предотвращения перехвата конфиденциальных данных (например, межсетевые экраны, защита паролем, шифрование и доступ третьих лиц со стороны облачных провайдеров)
2. **Метаданные и ESI** = Знание о непреднамеренном получении информации с метаданными и безопасность конфиденциальной информации, хранящейся в электронном виде, в процессе сбора и истребования доказательств и в ходе представительства клиентов.
3. **Е-поиск информации (E-discovery)** = Выполнение электронного поиска информации на основе федеральных и государственных правил, норм приема для электронного поиска информации, релевантности ESI и очистки метаданных или преобразования документов.
4. **Облачные вычисления (Cloud Computing)** = Знание облачных вычислений и систем хранения, доступа третьих сторон и разумных гарантий для хранения данных.
5. **Защита в Wi-Fi** = Основные условия безопасности, неиспользование общедоступного Wi-Fi, разумная защита/разумные защиты для предотвращения перехвата данных клиента и шифрование конфиденциальной информации клиента.

КАКИЕ ТЕХНОЛОГИЧЕСКИЕ НАВЫКИ ИМЕЮТСЯ?

6. **E-mail и Шифрование** = Знание зашифрованной и незашифрованной электронной почты, разумная защита для защиты конфиденциальной или высокочувствительной электронной почты клиента, а также последствия электронного обнаружения для практики.

7. **Виртуальные юридические фирмы** = Разумное электронное общение и точный маркетинг для клиентов, а также обязанность информировать клиентов на протяжении всего представления клиентов и понимание государственных этических норм для виртуального юриста.

8. **Социальные сети** = Знание инструментов социальных сетей, разработка политики юридической фирмы в отношении социальных сетей, понимание последствий электронного раскрытия информации и информированное согласие клиента (ов), когда это необходимо при рассмотрении дела.

9. **Цифровые документы** = Базовое управление цифровыми документами, использование эксперта вне области компетенции юриста, предотвращение перехвата, шифрование или защита паролем высокочувствительных данных и очистка документации для электронного обнаружения.

10. **Современные методы коммуникации** = Эффективные методы коммуникации в дополнение к традиционным нормам, включая текстовые сообщения, электронную почту, социальные сети и безопасные онлайн или облачные службы обмена сообщениями.

ЧТО ЮРИСТЫ ДОЛЖНЫ ОЦЕНИВАТЬ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ?

1. Передачу высокочувствительной или конфиденциальной информации по электронной почте или через незашифрованные электронные сообщения;
2. Отправку электронного письма на или с учетной записи, которой отправитель или получатель электронной почты делится с другими;
3. Отправку электронного письма клиенту, когда возможно, что третье лицо знает пароль к учетной записи электронной почты, или отдельному клиенту в учетной записи рабочей электронной почты этого клиента, особенно если электронное письмо касается трудового спора клиента с его работодателем;
4. Отправку электронного письма с общедоступного компьютера или взятого напрокат компьютера, или когда юрист знает, что электронные письма, которые он отправляет, читаются на общедоступном или взятом напрокат компьютере или в незащищенной сети;
5. Отправку электронного письма, если юрист знает, что получатель электронной почты получает доступ к электронной почте на устройствах, которые потенциально доступны для третьих лиц или не защищены паролем;
6. Отправку электронного письма, если юрист обеспокоен тем, что правоохранительные органы могут прочитать электронное письмо юриста, имея на это ордер или без него.

БЛАГОДАРИМ ВАС!