Авдалян А.А. Юридические аспекты в DFIR // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 10(48) с. 26–29

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЮРИДИЧЕСКИЕ АСПЕКТЫ В DFIR

Авдалян А.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: sharmanka228@gmail.com

Статья "Legal Considerations in DFIR" предоставляет всесторонний обзор юридических аспектов, связанных с цифровыми форензическими расследованиями и реагированием на инциденты (DFIR). В работе рассматриваются ключевые правовые вопросы, которые могут возникнуть в процессе сбора, анализа и представления доказательств в цифровых расследованиях. В статье освещаются важные темы, такие как соблюдение законодательства о конфиденциальности данных, соблюдение правил допустимости доказательств в суде и взаимодействие с правоохранительными органами. Автор также обсуждает юридические риски и рекомендации по минимизации правовых последствий, а также предоставляет практические советы для профессионалов в области DFIR.

Ключевые слова: Цифровая форензика, реагирование на инциденты, юридические аспекты, конфиденциальность данных, допустимость доказательств, правоохранительные органы, правовые риски, минимизация последствий, расследование, правовая ответственность.

LEGAL ASPECTS IN DFIR

Avdalyan A.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

The article "Legal Considerations in DFIR" provides a comprehensive overview of the legal aspects related to digital forensic investigations and Incident Response (DFIR). The paper examines the key legal issues that may arise in the process of collecting, analyzing and presenting evidence in digital investigations. The article highlights important topics such as compliance with data privacy laws, compliance with the rules of admissibility of evidence in court and interaction with law enforcement agencies. The author also discusses legal risks and recommendations for minimizing legal consequences, as well as provides practical advice for professionals in the field of DFIR.

Keywords: Digital forensics, incident response, legal aspects, data confidentiality, admissibility of evidence, law enforcement agencies, legal risks, minimization of consequences, investigation, legal responsibility.

Введение

В эпоху цифровых технологий и повсеместного использования информационных систем, вопросы цифровой безопасности и реагирования на инциденты (DFIR) приобрели особую значимость. Успешное проведение цифровых форензических расследований требует не только высокой квалификации в области технологий и методов сбора данных, но и глубокого понимания юридических аспектов, которые могут существенно повлиять на исход расследования и его правовые последствия.

Цифровая форензика занимается анализом электронных данных с целью выявления и документирования доказательств преступной деятельности или нарушения политики

безопасности. Однако, сбор и обработка таких данных требуют соблюдения строгих юридических норм и процедур, чтобы доказательства могли быть использованы в суде и не были признаны недопустимыми. Неправильное обращение с данными может привести к их порче, а также к юридическим последствиям, таким как санкции и репутационные потери.

Законодательство в области цифровой форензики постоянно эволюционирует, что требует от специалистов постоянного обновления знаний о правовых нормах, касающихся конфиденциальности данных, защиты личной информации и допустимости доказательств. Важными аспектами являются соблюдение требований по получению ордеров на обыск, правомерность доступа к данным и их анализ, а также соблюдение норм законодательства о защите данных, таких как Общий регламент по защите данных (GDPR) в Европе или Закон о защите персональных данных (CCPA) в США[2].

Данная статья нацелена на предоставление комплексного анализа юридических вопросов, связанных с DFIR, с акцентом на практические аспекты и рекомендации для профессионалов в этой области. Мы рассмотрим ключевые правовые принципы и практики, которые помогут избежать распространенных юридических ошибок и обеспечат успешное разрешение цифровых расследований.

Legal Considerations in DFIR

Законодательные основы и права доступа

Современные цифровые форензические расследования требуют строгого соблюдения законодательных норм, касающихся сбора и обработки данных. В различных юрисдикциях существуют законы, регулирующие доступ к цифровой информации и способы её получения. Например, в США часто используются ордера на обыск, которые дают правообладателям право доступа к электронным данным. В Европе правила, такие как Общий регламент по защите данных (GDPR), устанавливают ограничения на сбор и обработку персональной информации. Специалисты в области DFIR должны четко понимать и соблюдать эти нормы, чтобы избежать правовых последствий и обеспечить допустимость собранных доказательств в суде[3].

Принципы допустимости доказательств

Одним из ключевых аспектов в цифровых расследованиях является допустимость доказательств. Для того чтобы доказательства были признаны судом, они должны быть собраны и обработаны в соответствии с законами и стандартами. Это включает в себя обеспечение целостности данных, правильное документирование всех шагов процесса и соблюдение цепочки хранения доказательств. Профессионалы в области DFIR должны применять надлежащие методы для защиты доказательств от модификаций и утрат, чтобы сохранить их достоверность и обеспечить их принятие в суде.

Конфиденциальность и защита данных

Конфиденциальность данных является важным аспектом, требующим внимания в процессе цифровых расследований. Законодательства, такие как GDPR в Европе и Закон о защите персональных данных (CCPA) в США, обязывают организации обеспечивать защиту личной информации и уведомлять пользователей о сборе и обработке их данных. Специалисты в области DFIR должны гарантировать, что сбор данных осуществляется в рамках закона и что личная информация защищена от несанкционированного доступа.

Нарушение норм конфиденциальности может привести к значительным штрафам и юридическим последствиям[1].

Взаимодействие с правоохранительными органами

Правильное взаимодействие с правоохранительными органами имеет решающее значение для успешного проведения цифровых расследований. Специалисты должны быть готовы к сотрудничеству с правоохранительными органами, предоставляя им необходимые данные и документы в установленном формате. Это взаимодействие должно осуществляться в рамках правового поля и с соблюдением всех процессуальных норм. Также важно документировать все взаимодействия и обмен информацией с правоохранительными органами для обеспечения прозрачности и последующей проверки.

Примеры юридических рисков и решений

Примеры юридических рисков в DFIR включают неправильное обращение с данными, недостаточную документацию и нарушение конфиденциальности. Например, случай из практики, когда доказательства были признаны недопустимыми из-за недостаточной цепочки хранения, демонстрирует важность соблюдения всех требований. Для минимизации рисков рекомендуется внедрение четких процедур для сбора и обработки данных, регулярное обучение сотрудников и консультации с юридическими экспертами[4].

Рекомендации по соблюдению законодательства

Чтобы избежать юридических рисков и обеспечить успешное проведение цифровых расследований, следует придерживаться ряда рекомендаций. Во-первых, необходимо всегда получать соответствующие ордера и разрешения для доступа к данным. Во-вторых, важно обеспечить полное и точное документирование всех этапов расследования. В-третьих, следует регулярно обновлять свои знания о текущих изменениях в законодательстве и стандартам защиты данных. Также полезно иметь юридического консультанта для проверки и подтверждения соблюдения всех правовых требований[5].

Заключение

Правильное понимание и соблюдение юридических аспектов цифровых форензических расследований (DFIR) играют ключевую роль в обеспечении успешного и законного проведения расследований. Учет законодательных требований, связанных с доступом к данным, допустимостью доказательств и защитой конфиденциальности информации, а также грамотное взаимодействие с правоохранительными органами способствуют минимизации правовых рисков и укреплению доверия к результатам расследований. Для достижения наилучших результатов специалистам в области DFIR рекомендуется регулярно обновлять свои знания о правовых нормах и внедрять передовые практики, что поможет гарантировать соответствие законодательным требованиям и обеспечить надежность собранных доказательств.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.
4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. . Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data // High–tech technologies in Earth space research. – 2020. – Vol. 12. – No. 1. - pp. 70-76.
2. Minyaev A. A. Method for evaluating the effectiveness of an information protection system geographically distributed personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
3. Chmutov M. V. et al. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference proceedings. – 2017. – pp. 535-537.
4. Petrova T. V. et al. Approaches for detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to the classification of texts by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.