УДК 004.056.5

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И ПРОБЛЕМЫ ИХ РЕАЛИЗАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ДИСТАНЦИОННОГО ПРАВОСУДИЯ

© 2020 А. О. Бокова, Л. С. Михайлова

Российский государственный университет правосудия (г. Воронеж, Россия)

В статье рассматриваются методы защиты информации при осуществлении дистанционного правосудия и проблемы их реализации; методы несанкционированного доступа; меры, принятие которых необходимо для предупреждения несанкционированного доступа; применение видеоконференцсвязи в суде, ключевые особенности и осуществление дистанционного правосудия.

Ключевые слова: защита информации, методы защиты информации, несанкционированный доступ, видеоконференцсвязь, дистанционное правосудие.

Внедрение современных IT-технологий в работу судебных систем – один из наиболее эффективных способов повышения уровня доступности и качества правосудия в мире, способный ускорить процесс судопроизводства, сократить нагрузку на аппарат суда, повысить уровень открытости судебной системы, помочь сторонам экономить силы, время и деньги. Актуальность обеспечения информационной безопасности информационных систем судопроизводства обусловлена ростом компьютерных вторжений, существующей проблемой персонификации и безопасности доступа к информационным ресурсам судов.

Для обеспечения информационной безопасности судебной системы необходимо принятие мер по обеспечению компьютерной безопасности судов, криптографической защиты персональных данных в информационных системах судов, обработки данных; по защите информации от кибер-атак; по развитию электронной идентификации и других средств обеспечения безопасности и достоверности электронных судебных процедур [1].

Согласно теоретическим аспектам защиты информации при осуществлении удаленного взаимодействия по каналам связи следует выделить два основных блока. Это защита информации каналов связи Ethernet при помощи технических средств и защита информации при помощи программного обеспечения. Неудивительно, что распределённые сети подвергаются атакам, поскольку не нужно проникать внутрь защитного периметра, взламывать системы, искать в них данные: достаточно подождать, когда эти данные пройдут сами по сети, причём утечку данных через сеть как правило обнаружить довольно сложно.

Следует выделить ключевые особенности дистанционного правосудия, которые помогут сформировать подходящий набор методов для защиты информации применительно к подобному профилю [2, 3]:

- подключенных объектов (где под объектом будем понимать узел связи) между собой может быть 2 и более;
- объекты преимущественно находятся в глобальной сети;
- для связи объектов может быть использована спутниковая связь;
- передаваемая информация по каналам связи Ethernet представляет собой видео поток и звуковой поток;
- осуществляется запись видеоконференцсвязи.

Телекоммуникационная технология интерактивного взаимодействия абонентов, с возможностью обмена видеоинформацией в реальном масштабе времени и учётом передачи управляющих данных, широко применяется в различных сферах общественной жизни, в том числе при проведении судебного заседания. Применение видеоконференцсвязи в суде наряду с достоинствами имеет юридические и технические проблемы. Для пользования системой видеоконференцсвязи требуется техническое оснащение судов. Суд

Бокова Алёна Олеговна – Российский государственный университет правосудия, студент, a.o.bokova@gmail.com.

Михайлова Людмила Сергеевна – Российский государственный университет правосудия, старший преподаватель кафедры правовой информатики, информационного права и естественнонаучных дисциплин, mls55@mail.ru.

должен быть оснащён соответствующим оборудованием [4-6] и в нужный момент иметь возможность установить контакт с необходимым субъектом через каналы связи, отвечающие требованиям видеоконференции. В перспективе система видеоконференций позволит организовать сеансы для любых участников процесса, территориально удаленных друг от друга, что существенно сократит их финансовые и временные затраты [7].

Различные категории дел, рассматриваемые в судебном порядке, в той или иной мере, интересуют злоумышленников. Поэтому в случае рассмотрения резонансных дел посредством видеоконференцсвязи возникает вероятность несанкционированного доступа к информации.

Выделим основные методы несанкционированного доступа [8, 9]:

1. Несанкционированный доступ к информации, находящейся на физических носителях;
2. Преодоление любым из способов парольной защиты;
3. Использование багов в коде, для получения несанкционированного доступа к информации;
4. Внедрение любым из способов вредоносного программного обеспечения;
5. Использование методов социальной инженерии;
6. Использование аппаратных закладок;
7. Использование ненадёжного канала связи, осуществляющего небезопасную передачу информации.

Из приведённого перечня методов несанкционированного доступа к информации можно сделать вывод, что у злоумышленника достаточно обширный набор инструментов. Каждый из методов может быть реализован большим количеством способов, что усложняет разработку шаблонных рекомендаций по выработке мер средств защиты.

Представим перечень мер, необходимых для использования администратором по защите информации, которые должны в большей степени раскрывать методы защиты информации для сервисов видеоконференцсвязи и противостоять соответствующим методам несанкционированного доступа к ним.

Для предупреждения несанкционированного доступа к физическим носителям необходимо применить следующие меры:

- учёт машинных носителей информации, а также организация доступа к ним;
- осуществлять контроль используемых интерфейсов ввода (вывода);
- осуществлять контроль событий информационной безопасности, в частности их состав и содержание.

Для предупреждения несанкционированного доступа к сервису при помощи подбора пароля необходимо:

- применять длинные и сложные пароли, возможно использование скриптов для их генерации;
- блокировать учетные записи пользователей в случае выявления событий, являющихся потенциально несанкционированными;
- производить принудительную смену пароля для всех категорий пользователей;
- применять блокировку загрузки с незарегистрированных носителей;
- проводить регулярный аудит паролей.

Для предупреждения использования багов в программном коде необходимо принять следующие меры:

- своевременно обновлять программное обеспечение, в частности которое используется для сервиса видеоконференцсвязи;
- использовать официальное программное обеспечение.

Для предупреждения несанкционированного доступа при помощи внедрения вредоносного программного обеспечения необходимо принять следующие меры:

- использовать антивирусное программное обеспечение;
- проверять файлы на съёмных носителях;
- требовать от сотрудников организации соблюдать меры безопасности при использовании сети Интернет.

Для предупреждения несанкционированного доступа методов социальной инженерии необходимо:

- не раскрывать структуру и состав организации (данный пункт касается технических средств, состава программного обеспечения, организации локальной сети и т. д.);
- не опубликовывать личные данные сотрудников в открытых источниках;
- знать сотрудников организации, подразделений и филиалов.

Для предупреждения несанкционированного доступа от использования аппаратных закладок необходима периодическая проверка оборудования, а также разграничение доступа к объекту.

Для предупреждения несанкционированного доступа к сервису видеоконференцсвязи, использующему ненадежный канал связи, необходимо:

- использовать специализированные средства VPN;
- использовать криптографические методы защиты информации;
- правильно настроить оборудование [10, 11].

Выделим среди приведённых меры, которые можно определить как общие:

- контроль состава технических средств, программного обеспечения и средств защиты информации;
- контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
- контроль целостности программного обеспечения, включая программного обеспечение средств защиты информации.

Необходимо учитывать тот факт, что в гражданском и уголовном судопроизводстве дела, связанные с участием в заседании несовершеннолетних, вопросами усыновления и удочерения, необходимостью защиты государственной и иных видов тайн, главой 18 УК РФ, характеризуются как дела, которые принято рассматривать только в закрытом судебном заседании [12, 13]. Это означает, что в процессах данной категории дел участвуют только стороны, прокуратура, и, при необходимости, представители территориальных органов (отдел опеки и попечительства при установлении усыновления или удочерения). В связи с конфиденциальностью данных вопросов, техническую сторону проведения судебного заседания необходимо усилить дополнительными средствами защиты информации.

Цифровизация судебной системы в период ограничений, связанных с коронавирусом, существенно продвинулась вперёд, поскольку альтернативы для проведения заседаний в ином формате не существовало.

По мнению независимого советника по правовым вопросам Павла Петровича Гейко, вопрос информационной безопасности имеет фундаментальное значение, поскольку «для значительного числа IT-специалистов сегодня ничего не стоит подменить вложения, которые направляются по обычным каналам связи. Создать подделку документа и направить его в суд ничего не стоит, а с учётом быстрого «шаблонного» правосудия риск вынесения на основе такого документа неправосудного решения очень велик».

Таким образом, на основании вышеизложенного, а также учитывая мнение экспертов-юристов, полагаю, что для качественной работы «дистанционного правосудия» необходима грамотная техническая реализация и неукоснительное соблюдение требований к защите информации.

ЛИТЕРАТУРА

1. Бокова А. О. Проблемы организации видеоконференцсвязи в суде / А. О. Бокова // Всероссийская научно-практическая конференция «Актуальные вопросы эксплуатации систем охраны и защищённых телекоммуникационных систем» : сборник материалов. – Воронеж : Воронежский институт МВД России, 2020. – С. 13-16.

2. Рогозин Е. А. Методика исследования вероятностно-временных характеристик реализации сетевых атак в программной среде имитационного моделирования / И. Г. Дровникова, А. А. Змеев, А. Д. Попов, Е. А. Рогозин // Вестник Дагестанского государственного технического университета. Технические науки. – Махачкала, 2017. – 44 (4). – С. 99-113.

3. Губанов А. В. Обеспечение конфиденциальности информации в ведомственных системах видеоконференцсвязи / А. В. Губанов // Телекоммуникационные системы и компьютерные сети. – Москва, 2010. – С. 309-312.

4. Миронов А. Н. Использование системы видеоконференцсвязи в судебной деятельности / А. Н. Миронов, Ю. В. Миронова // Российский судья. – Москва, 2019. – № 7. – С. 22-26.

5. Приказ Судебного департамента при Верховном Суде РФ от 28.12.2015 № 401 «Об утверждении Регламента организации применения видеоконференцсвязи в федеральных судах общей юрисдикции» // КонсультантПлюс. – URL: http://www.consultant.ru/cons/_doc_LAW_8982.htm (дата обращения: 09.11.2020).

6. Приказ Судебного департамента при Верховном Суде РФ от 08.08.2019 № 174 «О внесении изменений в Регламент организации применения видеоконференцсвязи в федеральных судах общей юрисдикции, утвержденный приказом Судебного департамента от 28 декабря 2015 г. № 401» / Гарант. – URL: https://www.garant.ru/products/ipo/prime/doc/72662240.htm (дата обращения: 09.11.2020).

7. Уголовно-процессуальный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 02.08.2019) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

8. Абидарова А. А. Физические средства защиты информации / А. А. Абидарова // Наука, образование и культура. – 2019. – № 2 (36). – С. 19-20.

9. Образумов Е. И. Защита информационных ресурсов от несанкционированного доступа / Е. И. Образумов, А. Ю. Сергеев // Экономическая безопасность общества, государства и личности: проблемы и направления обеспечения: сборник статей по материалам VI научно-практической конференции. – Прага: Vědecko vydavatelské centrum "Sociosféra-CZ", 2019. – С. 113-116.

10. Приказ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21.htm (дата обращения: 09.11.2020).

11. Каторин Ю. Ф. Защита информации техническими средствами : Учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак // Санкт-Петербург: НИУ ИТМО, 2012. – 416 с.

12. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ (ред. от 27.10.2020) // Собрание законодательства Российской Федерации. – 1996. – Гл. 18. – Ст. 131-135

13. Гражданский процессуальный кодекс Российской Федерации от 14. нояб. 2002 № 138-ФЗ (ред. от 31.07.2020) // Собрание законодательства Российской Федерации. – 2002. – ГЛ. 29. – Ст. 269-275.

INFORMATION PROTECTION METHODS AND THE PROBLEMS OF THEIR IMPLEMENTATION IN THE IMPLEMENTATION OF REMOTE JUSTICE

© 2020 A. O. Bokova, L. S. Mikhailova

Russian State University of Justice (Voronezh, Russia)

The article deals with information protection methods in the implementation of remote justice and problems of their implementation; methods of unauthorized access; measures, the adoption of which is necessary to prevent unauthorized access; application of video conferencing in court, key features and implementation of remote justice.

Keywords: information security, information security methods, unauthorized access, video conferencing, remote justice.