Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2024-3-70-85

КЛЮЧЕВЫЕ АСПЕКТЫ РАЗРАБОТКИ МЕЖДИСЦИПЛИНАРНОЙ МЕТОДИКИ ДЛЯ ВНУТРЕННИХ РАССЛЕДОВАНИЙ КИБЕРПРЕСТУПЛЕНИЙ

✉Чечулин Андрей Алексеевич;
Горда Максим Дмитриевич;
Котов Александр Александрович.
Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия
✉andreych@bk.ru

Аннотация. Сформулированы требования к разработке междисциплинарной методики внутреннего расследования киберпреступлений. На основе анализа релевантных работ, а также проблем каждой из областей (технической и юридической) разрабатываются требования, учитывающие недостатки существующих подходов. Сформированные требования будут использованы для разработки междисциплинарной методики внутреннего расследования киберпреступлений в российских организациях. Научная новизна заключается в междисциплинарном подходе, который авторы формируют впервые в области исследования. Практическая новизна разработанного решения заключается в возможности применения результатов статьи в коммерческих и бюджетных организациях России для разработки внутренней документации, построения эффективного процесса расследования, а также анализа существующих подходов к расследованию внутренних инцидентов на предмет корректности с юридической и технической стороны одновременно. Данная статья является первой в цикле статей по разработке методики расследования.

Ключевые слова: информационная безопасность, расследования кибератак, внутренние расследования, форензика

Для цитирования: Чечулин А.А., Горда М.Д., Котов А.А. Ключевые аспекты разработки междисциплинарной методики для внутренних расследований киберпреступлений // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 70–85. DOI: 10.61260/2218-13X-2024-3-70-85.

Scientific article

KEY ASPECTS OF DEVELOPING AN INTERDISCIPLINARY METHODOLOGY FOR INTERNAL CYBERCRIME INVESTIGATIONS

✉Chechulin Andrey A.;
Gorda Maxim D.;
Kotov Alexander A.
Saint-Petersburg federal research center of the Russian academy of sciences, Saint-Petersburg, Russia
✉andreych@bk.ru

Abstract. In this article, the requirements for the development of an interdisciplinary methodology for internal cybercrime investigations are formulated. Based on the analysis of relevant works, as well as the problems of each area (technical and legal), requirements are being developed that take into account the shortcomings of existing approaches. The formed requirements will be used to develop an interdisciplinary methodology for internal cybercrime investigation in Russian organizations. The scientific novelty lies in the interdisciplinary approach that the authors are forming for the first time in the field of research. The practical novelty of the developed

© Санкт-Петербургский университет ГПС МЧС России, 2024

solution lies in the possibility of applying the results of the article in commercial and budgetary organizations of Russia for the development of internal documentation, building an effective investigation process, and analyzing existing approaches to investigating internal incidents for correctness from both a legal and technical perspective at the same time. This article is the first in a series of articles on the development of an investigation methodology.

Keywords: information security, cyber-attack investigations, internal investigations, forensics

For citation: Chechulin A.A., Gorda M.D., Kotov A.A. Key aspects of developing an interdisciplinary methodology for internal cybercrime investigations // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 70–85. DOI: 10.61260/2218-13X-2024-3-70-85.

Введение

В эпоху цифровизации и постоянного роста количества и разнообразия киберугроз актуальность вопросов информационной безопасности для всех организаций становится всё более очевидной. Бюджетные организации, как и коммерческие структуры, подвергаются риску нарушений в этой сфере, однако их специфика диктует особые условия и подходы к расследованию инцидентов и приводит к тому, что анализ инцидентов не может быть проведен только техническими специалистами без учета правовых особенностей этого процесса. Это может быть более строгая регламентация, особенности финансирования, а также специфические требования к уровню безопасности и порядку обработки государственной информации. Таким образом, подходы к расследованию и реагированию на инциденты в российских организациях требуют особого внимания и компетентности.

При этом для бюджетных организаций значимость расследований инцидентов информационной безопасности особенно велика, так как от их результативности может зависеть не только сохранность конфиденциальных данных государственного значения, но и доверие граждан к государственным институтам.

Научная новизна данной работы заключается в междисциплинарном подходе к разработке требований для проведения внутренних расследований инцидентов информационной безопасности в российских организациях. Кроме того, в статье проведен совместный анализ технических и юридических решений в этой области, что также отличает её от существующих исследований.

Практическая значимость результатов статьи заключается в возможности их использования для оценки корректности текущих процессов внутренних расследований киберпреступлений и выявления потенциальных проблем. Кроме того, результаты исследования могут служить основой для разработки новых междисциплинарных решений и внутренних регламентов, направленных на эффективное расследование инцидентов информационной безопасности.

Предлагаемый в данной статье анализ юридических и технических особенностей внутренних расследований позволяет сформировать комплексный взгляд на процесс расследования, что становится ключом к эффективной и своевременной реакции организации на инциденты информационной безопасности.

Методы исследования

Тематика расследования киберпреступлений является востребованной в современном научном мире. Она касается как технических, так и юридических аспектов процесса расследования. Несмотря на большое количество частных криминалистических методов и подходов, не все они учитывают обе эти стороны. Авторы релевантных работ обращают своё внимание на несовершенство существующих подходов к реализации данного процесса.

Например, в своей статье [1] А.С. Шаталов раскрывает тему популярности киберпреступлений в России и в мире в целом. Автор объясняет данный феномен большой прибыльностью преступлений в области компьютерной информации и низким риском разоблачения преступника правоохранительными органами, что в совокупности является привлекательным для потенциальных правонарушителей. Шаталов А.С. обращает внимание на то, что с течением времени всё больше преступлений уходит в цифровое пространство, тем самым становятся более актуальными новые методы предотвращения подобного рода преступлений. Также в статье обращается внимание на возможные последствия неверно собранных доказательств сотрудниками-криминалистами, что может повлечь за собой некорректное представление фактов киберпреступлений в суде или отказ суда принимать неверно собранные цифровые следы правонарушения. Авторы видят решение данных проблем в применении методов систематизации уже существующих работ в области цифровой криминалистики и разработке новых методов проведения процессов, связанных с расследованием преступлений в области компьютерной информации.

Вершицкая Г.В. [2] проводит классификацию следов в качестве источников информации о киберпреступлении. Особое внимание обращается на возможную недостоверность цифровой информации, полученной в результате сбора следов киберпреступления. Также определяется проблема недолговечности следов киберпреступления и проблема недостаточного уровня изучения видов преступлений, совершаемых с использованием информационных технологий. Исходя из этих проблем, автор статьи выделяет недостаток практического опыта субъектов криминалистической деятельности по раскрытию и расследованию данной категории преступлений, а также отсутствием у них специальных знаний в области информационных технологий. Авторы обращают внимание, что данные на этапе сбора должны быть собраны согласно требованиям уголовно-процессуального законодательства, что показывает важность корректного сбора такого вида информации. Для решения определенных в статье проблем предлагаются следующие методы: установление на законодательном уровне правил сбора, исследования и оценки цифровых доказательств; разработка приемов, методов и средств сбора и исследования цифровых доказательств.

Авторы статьи [3] обращают внимание на возникающие проблемы при расследовании киберпреступлений специалистами правоохранительных органов. На основе данного положения формируется проблема разработки криминалистической методики и тактики раскрытия преступлений в области компьютерной информации. Для формирования основы будущих тактик и методик, авторы приводят в пример следственно-экспертные ситуации, в которых они могут быть использованы, а также формируют особенности преступлений в области компьютерной информации. Используя методы анализа существующих практических следственных ситуаций, в которых частично доказательства имели цифровой вид на данный момент, авторы делают вывод о необходимости взаимодействия сотрудника правоохранительных органов со специалистом-экспертом в области форензики не только в процессе компьютерно-технической экспертизы, а на всех этапах расследования.

Однако, учитывая ограниченности ресурсов экспертов в области форензики, не для каждого киберпреступления можно нанять специалиста, который будет его расследовать. В рамках проведения внутренних расследований, результаты данной статьи можно использовать с технической точки зрения, однако юридические особенности тоже требуют особого внимания.

В своей статье [4] О.А. Решняк обращает внимание на сложность расследования киберпреступлений в связи с постоянно меняющимися способами их совершения. На основе приведённых автором примеров совершения киберпреступлений формируется проблема, которая заключается в минимальном количестве криминалистической значимой информации в результате совершения злоумышленниками преступных действий. Решением проблем, обозначенных в статье, по мнению О.А. Решняк, может являться совершенствование частных криминалистических методик расследования, а также разработки новых методов

взаимодействия правоохранительных органов с организациями, которые могут предоставить необходимые данные. Представляется, что предложенные меры будут способствовать повышению эффективности расследования преступлений.

Однако криминалистическая методика должна включать технические и юридические аспекты расследования, так как даже в минимальном количестве значимой криминалистической информации может быть та, которую невозможно собрать с юридической точки зрения. Такой подход позволит более комплексно и эффективно построить процесс расследования.

Авторы статьи [5] обращают внимание на важность цифровой криминалистики при расследовании преступлений в современном мире. Также в статье обращается внимание на сложность извлечения цифровых данных из-за особенностей процесса сбора, извлечения и большого объёма гетерогенных данных. Обращая внимание на несовершенство Уголовно-процессуального кодекса Российской Федерации (УПК РФ) в сфере цифровых доказательств, авторы констатируют факт затруднения получения доступа к цифровой информации в процессе расследования уголовных дел. Они приходят к выводу о необходимости разработки методов применения цифровых доказательств в процессе расследования, так как цифровые технологии дают значительные возможности для эффективного раскрытия и расследования преступлений.

Такая практика применима и к внутренним расследованиям киберпреступлений, цифровые доказательства в которых могут иметь решающую роль. Однако, несмотря на мнение авторов о несовершенстве законодательства в данной сфере, необходимо построить процессы таким образом, чтобы они были применимы как с технической, так и с юридической точки зрения, особенно на первых этапах при сборе необходимых гетерогенных данных.

Шушеначев А.В [6] выделяет признаки цифровой информации, которые являются существенными в процессе ее трансформации в доказательства электронного типа. Затем, на основе выделенных критериев определяет необходимые этапы процесса сбора в соответствии с законодательством России, тем самым применяя методы систематизации. Также автор статьи обращает внимание на необходимость привлечения к сбору цифровых доказательств квалифицированных специалистов. На основе положений УПК РФ формируются требования к специалисту и к его действиям в процессе сбора доказательств, так как изъятие устройства не всегда представляется возможным. Автор проводит анализ двух методов сбора информации: копирование и изъятие физических носителей и приходит к выводу, что оба метода имеют свои преимущества и недостатки и должны использоваться в зависимости от возникающих в ходе расследования задач.

Для построения эффективного процесса расследования внутренних инцидентов необходимо сопоставить каждый из технических этапов расследования с юридической составляющей, чтобы специалист, использующий научный результат, мог быть уверен в своих действиях при сборе, извлечении, анализе и представлении доказательств.

Обзор релевантных работ показал, что тема построения корректного процесса расследования внутренних киберпреступлений является актуальной на данный момент. Авторы, с одной стороны, дискутируют по поводу несовершенства технических методов расследования, с другой стороны, не все из них рассматривают юридическую составляющую самого процесса. Однако это, несомненно, важная тема, так как правовая составляющая процесса внутренних расследований влияет на информацию, которую может собрать специалист, тем самым влияет на результаты расследования, что влечёт за собой влияние на эффективность всего процесса.

В статье на основе анализа релевантных работ в области расследования киберпреступлений из двух областей (технической и юридической) будет проводиться систематизация накопленного научного опыта с целью получения междисциплинарного результата. Будут использованы методы и подходы из обеих областей, и на основе анализа проблематики технического и юридического подхода к расследованию будут

сформулированы рекомендации к построению новой междисциплинарной методики, которая позволит эффективнее построить процесс расследования за счёт получения большего количества необходимой информации в процессе её применения.

Основные технические этапы внутреннего расследования инцидентов информационной безопасности

Основными техническими этапами расследования киберпреступлений являются: сбор информации о зарегистрированном инциденте, извлечение доказательств, анализ полученных доказательств, формирование выводов и предоставление рекомендаций. Результат каждого предыдущего этапа передается на вход последующему, так как на первом этапе происходит сбор информации, из которой в дальнейшем извлекаются факты о киберпреступлении. Далее факты анализируются на предмет причастности к инциденту и систематизируются для представления их в виде финального отчёта. Опишем более подробно каждый из этапов.

Сбор информации

На первом этапе расследования сотрудники отдела информационной безопасности (или иного отдела, на который возложены такие обязательства) определяют, принадлежат ли отдельные инциденты к инцидентам информационной безопасности. В каждой организации есть свои методики и способы отнесения к инцидентам, которые в дальнейшем необходимо расследовать. В основном при получении первичных данных их относят или не относят к различным классификациям атак и их признаков.

В данной статье под инцидентами информационной безопасности понимаются любые события или действия, которые приводят к нарушению конфиденциальности, доступности или целостности информации, хранящейся в организации. Кроме угроз для информации инциденты безопасности могут включать перехват управления над программной или аппаратной инфраструктурой организации, распространение вредоносных программ и другие виды.

Информация об инциденте может поступить из различных источников, например:

– системы мониторинга инцидентов;

– сотрудники организации;

– результаты аудитов информационной безопасности и т.д.

Далее осуществляется сбор первичной информации (сырых данных) об инциденте. Сбор данных начинается с технических средств, собирающих журналы инцидентов безопасности. Также на этом этапе собираются метаданные и определяются те события или данные, которые относятся к расследуемому инциденту безопасности.

После сбора данных с технических средств проводятся опросы сотрудников, с которых была затронута атака, для выяснения дополнительных векторов атак злоумышленников, которые могут позволить собрать еще больше данных для успешного расследования атаки.

Извлечение доказательств

Следующим этапом расследования киберпреступлений будет являться извлечение информации, которая необходима для выяснения целей методов и последствий атаки, а также для расследования и анализа инцидента безопасности. В свою очередь, цифровые доказательства представляют собой электронные данные, которые могут быть использованы в качестве фактов в юридическом процессе. Эти данные могут включать в себя журналы операционных систем и других программ, электронную почту, элементы файловой системы, а также любые другие цифровые следы действий злоумышленников.

Анализ полученных данных

На данном этапе проводится анализ технических методов злоумышленника. Такими методами могут быть фишинговые письма, вредоносные вложения, различные виды атак, использование специализированного программного обеспечения и т.д.

На основе анализа собранных данных формируются выводы об источнике атаки и целях злоумышленников. Полученные данные могут помочь составить круг сотрудников (или технических средств), которых затронула (или потенциально затронула) атака, тем самым будут определены цели злоумышленников. Собранные метаданные помогут выяснить источники атаки или их примерную геопозицию.

После определения целей и источников атаки анализируются техники и подходы злоумышленников для определения вредоносных действий и формирования рекомендаций для предотвращения подобного вида атак в будущем; векторы атаки злоумышленников, которые могут позволить уточнить круг затронутых атакой активов, а также предотвратить потенциальные атаки на «будущие» цели.

Также, чтобы корректно идентифицировать атаку, необходимо, на основе анализа собранных данных, найти ключевые особенности атаки, которые позволят либо объединить информацию в один инцидент, либо разделить на разные.

Формирование выводов и предоставление рекомендаций

Последним этапом расследования киберпреступления будет являться формирование выводов и предоставление рекомендаций. На данном этапе на основе собранной и проанализированной информации делается вывод об успешности атаки, а также о количестве затронутых активов в организации. Также исходя из полученных данных о целях, векторах, методах злоумышленников, производится оценка ущерба от инцидента информационной безопасности. Оценка ущерба включает в себя как финансовый, так и репутационный аспект.

После формирования выводов и оценки ущерба проводятся профилактические мероприятия, направленные на повышение защищенности активов организации, а также на повышение информированности сотрудников организации об актуальных видах атак и на то, как не стать их жертвой. Рекомендации должны включать в себя методы восстановления после успешных фактов совершения атаки [7, 8].

Проблематика юридически-корректного расследования

Для расследования внутренних инцидентов часто необходимо собрать большое количество гетерогенных данных, которые могут быть доказательством вредоносного воздействия на активы. Несмотря на корректный сбор информации о киберпреступлении с технической точки зрения, необходимо также учитывать юридическую сторону данного процесса. Отсутствие организационно распорядительной документации в организации, в которой проводится расследование может наложить ограничения на корректный сбор доказательств, что может повлиять на процесс расследования, а также на его результаты. Некоторую информацию нельзя собирать даже при необходимых принятых документах или только с согласия сотрудников. С одной стороны, юридические ограничения могут значительно сократить количество собираемой информации. С другой стороны, корректно собранные данные позволяют представить их в суде при доказательстве виновности потенциального правонарушения.

Существующие технические решения в области форензики не учитывают следующие юридические аспекты:

– правомерность сбора информации специалистами;

– категории информации, разрешенные для сбора в процессе расследования;

– обязанность уведомления контролирующих органов об инциденте и результатах расследования;

– ответственность за нарушение законодательства страны, в которой проводится расследование.

Тем самым, даже имея технически-корректный процесс расследования киберпреступления, можно не достигнуть необходимых результатов, а именно: процесс сбора данных может проводиться с нарушением законодательства, что не позволит представлять их в компетентных органах; в процессе действий специалистов могут быть собраны недопустимые с точки зрения законодательства данные, что впоследствии может привести к нелегитимности результатов расследования в юридической плоскости. Поэтому в процессе внутреннего расследования киберпреступлений необходимо учитывать не только технические, но и юридические аспекты.

Юридические аспекты внутренних расследований в российских организациях

Многие общие и частные решения в области расследования киберпреступлений подробно описывают технические требования к алгоритму действий специалиста по информационной безопасности, однако в подавляющем количестве случаев не учитывают юридические требования. Нормативные акты Российской Федерации устанавливают как ограничения для специалистов и для процесса расследования, так и административную и уголовную ответственность за их несоблюдение. В данном разделе будут описаны основные требования и ограничения, которые затрагивают процесс внутреннего расследования киберпреступлений в российских организациях.

Ограничения прав расследователей

Нормативная база содержит несколько ключевых режимов данных, которые могут быть затронуты при проведении внутреннего расследования в отношении – работодатель –> сотрудники для установления причин и последствий инцидентов информационной безопасности:

Согласно Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ФЗ № 152-ФЗ):

1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Также внутри режима персональных данных предусмотрено несколько специальных режимов, а именно:

1.1. Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом.

1.2. Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

1.3. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

1.4. Персональные данные работников – персональные данные физических лиц, вступивших в трудовые отношения с работодателем.

Помимо этого в российском законодательстве предусмотрены дополнительные режимы, защищающие данные сотрудников. К ним относятся:

2. Тайна частной и семейной жизни – любая информация о частной или семейной жизни субъекта, для которой предусмотрены специальные способы защиты, ограничения

на её использование (ч. 1 ст. 23, ч. 1 ст. 24 Конституции Российской Федерации, ст. 152.2 Гражданского кодекса Российской Федерации (ГК РФ) и ответственность.

3. Тайна связи – любая информация, содержащаяся в приватной коммуникации в разных видах (электронная, почтовая и т.д.) между лицами, а также информация о факте их коммуникации (ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»).

4. Компьютерная информация – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (ст. 272 Уголовный кодекс Российской Федерации).

Осуществляя сбор и иную обработку данных об инциденте информационной безопасности, работодатель (применительно к данной статье бюджетное учреждение) и лица, осуществляющие внутреннее расследование, обязаны учитывать эти режимы данных, чтобы не нарушить права сотрудников при проведении внутреннего расследования. Для каждого из режимов данных необходимо учитывать наличие правового основания, которое позволяет правомерным образом обрабатывать данные, связанные с сотрудниками. Кроме того, необходимо учитывать ограничения, которые установлены трудовым законодательством, а именно: 1) все персональные данные необходимо получать от сотрудника непосредственно либо по письменному согласию, предоставленному работником заранее; 2) не принимать решения, затрагивающие интересы работника, исключительно на основании автоматизированной обработки персональных данных или электронного получения; 3) защита персональных данных работника осуществляется за счет средств работодателя; 4) работники не должны отказываться от своих прав на сохранение и защиту данных; 5) осуществлять передачу персональных данных работника в пределах организации в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись; 6) разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения работником трудовых функций; 7) в случае передачи данных за пределы организации необходимо получить письменное согласие сотрудника либо использовать ограниченный перечень правовых оснований, связанных с взаимодействием с государственными органами или безопасностью сотрудников.

Правовые основания для проведения расследования

В качестве ключевых оснований обработки данных сотрудников для целей проведения внутреннего расследования сотрудника выступают: 1) согласие субъекта и (или) 2) выполнение возложенных законодательством Российской Федерации на работодателя функций, полномочий и обязанностей и (или) 3) законный интерес работодателя и (или) 4) исполнение договора.

Применительно к обработке данных сотрудников необходимо отметить, что законодателем установлено общее ограничение по целям обработки для всех случаев. В соответствии с п.п. 1 ст. 86 Трудового кодекса Российской Федерации (ТК РФ) обработка персональных данных может осуществляться работодателем лишь с целью обеспечения соблюдения нормативных правовых актов, содействия работникам в трудоустройстве, обучения и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

В этой связи согласие на обработку персональных данных не может предусматривать целей, которые выходят за пределы, установленные законодателем. То есть даже если согласие будет содержать избыточный набор данных применительно к заявленной цели, и работник его предоставит, это не значит, что оно будет являться действительным в этой части. Кроме того, к согласию применяются следующие требования – оно должно быть дано субъектом свободно, своей волей и в своем интересе; согласие должно быть конкретным (должны быть определены границы обработки), предметным (обработка данных должна

соотноситься с деятельностью оператора) информированным (субъекту должна быть предоставлена необходимая информация, предусмотренная законом), сознательным (должны быть определены конкретные цели обработки) и однозначным (бездействие не признается согласием).

Обработка персональных данных на основании п.п. 2 п. 1 ст. 6 ФЗ № 152-ФЗ (выполнение возложенных законодательством Российской Федерации на работодателя функций, полномочий и обязанностей) в контексте неправомерной передачи персональных данных подразумевает у оператора наличие обязанности по принятию мер реагирования на инцидент информационной безопасности. Чвсть 3.1. ст. 21 ФЗ № 152-ФЗ возлагает на оператора персональных данных обязанность по проведению внутреннего расследования и уведомлению Роскомнадзора о результатах. При этом закон предусматривают эту обязанность как для случаев неправомерной передачи, так и для случайной передачи, которая может выражаться в предоставлении, распространении, доступе к персональным данным.

Подзаконное регулирование устанавливает следующий перечень данных, которые оператор обязан передать о лицах, чьи действия стали причиной утечки в Роскомнадзор. Абзац 2 ч. 3 приказа Роскомнадзора от 14 ноября 2022 г. № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных» устанавливает, что к таким сведениям относятся: ФИО сотрудника и его должность, если причиной инцидента стали его действия. Кроме того, если учреждение относится к субъектам критической инфраструктуры, то ему необходимо дополнительно передать уведомление по системе ГосСОПКА в Федеральную службу безопасности в течение 24 ч, если произошла компьютерная атака.

Следует обратить внимание на тот факт, что в норме не предусмотрено, что работодатель вправе обрабатывать лишь этот перечень данных для проведения расследования. Только для передачи данных в Роскомнадзор (один из способов обработки персональных данных) законодатель предусмотрел ограничение, но в контексте проведения внутреннего расследования не обозначил, какие данные работодатель вправе обрабатывать, используя данное правовое основание. Вероятно, это является квалифицированным умолчанием со стороны законодателя, ведь для того, чтобы установить виновное лицо, явно недостаточно использовать информацию о ФИО и должностях сотрудников. Так как данная норма была введена в 2022 г., практика или подробные разъяснения со стороны Роскомнадзора отсутствуют. В связи с этим получается, что работодатель сам должен соотносить с целями соразмерность объемов обработки персональных данных для выполнения данной обязанности. Кроме того, данная обязанность вытекает из нормы, направленной на обработку персональных данных после того, как инцидент информационной безопасности произошел.

Применительно к законному интересу, необходимо отметить следующее. ТК РФ предусматривает возможность обработки работодателем данных для целей защиты собственного имущества и обеспечения личной безопасности работников. В случае с инцидентами информационной безопасности имущество работодателя находится в состоянии непосредственной угрозы, как и личная безопасность сотрудников, если их персональные данные будут использованы злоумышленниками в противоправных целях. Кроме того, в ТК РФ предусматривается правомочие работодателя по осуществлению фото, видео, аудио-фиксации процессов производства работ (ст. 214.2 ТК РФ), обеспечению дистанционного работника средствами защиты информации (ст. 312.6 ТК РФ), что является частью действий, направленных на превентивную защиту и реакционные действия в случае возникновения инцидента информационной безопасности.

Обработка персональных данных работников для целей исполнения трудового договора возможна с соблюдением ограничений по целям и обычно сводится к объему данных, предусмотренных формой Т-2 (Личная карточка работника), хоть она и носит

рекомендательный характер с 2013 г. Форма подразумевает заполнение следующих полей: ФИО, дата рождения, гражданство, профессия, паспортные данные, адрес места жительства, номер телефона и иные данные, предусмотренные формой. Эти данные также могут быть использованы при внедрении мер противодействия инцидентам информационной безопасности и реагировании на него.

Ответственность в случае неправомерной обработки данных сотрудников

В случае неправомерной обработки данных о работнике, которые покрываются режимами, описанными в п. 3.2 настоящей статьи, существует три потенциальных субъекта: 1) учреждение; 2) лицо, ответственное за организацию обработки персональных данных; 3) иные лица в организации, осуществившие неправомерную обработку персональных данных.

В рамках административной ответственности за неправомерную обработку персональных данных учреждение может быть оштрафовано на сумму до 150 тыс. руб. (при повторном нарушении до 500 тыс. руб.). Должностное лицо может быть оштрафовано на сумму до 40 тыс. руб. (при повторном нарушении до 100 тыс. руб.). Основание: ч. 1–1.1. или ч. 2–2.2. ст. 13.11 Кодекс Российской Федерации об административных правонарушениях.

В качестве гражданской ответственности за нарушение неприкосновенности частной жизни сотрудники вправе потребовать компенсации морального вреда. Основание: ст. 152.2 ГК РФ. Обычно суд взыскивает компенсацию в размере 10 000 руб. Кроме того, работники, виновные в нарушении законодательства о персональных данных, могут быть привлечены к дисциплинарной и материальной ответственности работодателем, вплоть до увольнения – ст. 90 ТК РФ.

Уголовное законодательство предусматривает набор составов, которые могут быть применены в случае неправомерной обработки персональных данных к указанным субъектам, за исключением бюджетной организации. К составам относятся: 1) нарушение неприкосновенности частной жизни – штраф до 300 тыс. руб. или лишение права занимать определенную должность, заниматься определенной деятельностью на срок до пяти лет или лишение свободы сроком до четырех лет или иные санкции, предусмотренные ч. 2 ст. 137 Уголовного кодекса Российской Федерации (УК РФ); 2) нарушение тайны связи – штраф до 300 тыс. руб. или лишение права занимать определенную должность, заниматься определенной деятельностью на срок до пяти лет или лишение свободы сроком до четырех лет или иные санкции, предусмотренные ч. 2 ст. 138 УК РФ; 3) неправомерный доступ к компьютерной информации – штраф до 500 тыс. руб. лишение права занимать определенную должность, заниматься определенной деятельностью на срок до трех лет или лишение свободы сроком до пяти лет, или иные санкции, предусмотренные ч. 3 ст. 272 УК РФ. Эти составы могут образовывать идеальную совокупность, что означает нарушение одним действием нескольких составов преступления – ч. 2 ст. 17 УК РФ, если противозаконно получен доступ к сведениям, составляющим тайну частной и семейной жизни [9].

Проблематика технически-корректного расследования

Таким образом, процесс внутренних расследований киберпреступлений имеет достаточно большое количество юридических ограничений в рамках российского законодательства. Также, помимо ограничений, нормативные акты регламентируют ответственность за их нарушение или частичное несоблюдение. Игнорируя нормы законодательства в рамках внутреннего расследования, организации и специалисты по информационной безопасности подвергают риску нелегитимности результаты расследования, а также в некоторых случаях могут быть привлечены к административной, уголовной и иным видам ответственности. С другой стороны, часто, отсутствие требований

со стороны законодательства к разработчикам программного и аппаратного обеспечения встраивать в свои разработки элементы журналирования приводит к отсутствию необходимой для анализа информации и также сокращает область для последующего проведения расследований [10].

Однако научные юридические решения зачастую не включают в себя технических аспектов, тем самым невозможно полноценно использовать их в практической деятельности специалистов по расследованию внутренних инцидентов. Такие решения в основном не учитывают:

– технические этапы расследования;

– особенности технического взаимодействия с программными и аппаратными частями объектов расследования;

– особенности использования специализированного программного обеспечения на различных этапах расследования;

– особенности фиксации цифровых доказательств.

Отсутствие технических научных знаний у специалиста, при необходимой юридической грамотности в данной области, может не позволить ему корректно провести процесс внутреннего расследования киберпреступления. Помимо знания юридических ограничений, специалистам важно понимать техническую часть процесса расследования, так как юридические нормы и стандарты, а также научные решения на данный момент недостаточно описывают технические аспекты расследования внутренних инцидентов. Таким образом, важно в процессе расследования использовать не только разработанные юридические решения и нормативные акты, но и учитывать технические аспекты в практической деятельности специалистов [11].

Требования к разработке методики юридически и технически корректного проведения внутренних расследований

В первую очередь учреждению необходимо обеспечить наличие правового основания и условий для обработки данных, чтобы соблюсти ограничения, предусмотренные режимами, перечисленными в п. 3.2 настоящей статьи. Учитывая, что стратегия противодействия информационным инцидентам подразумевает как превентивные (защита от потенциального инцидента информационной безопасности), так и реактивные действия (противодействие происходящему или произошедшему инциденту информационной безопасности), разумно использовать комбинацию из правовых оснований для обработки персональных данных, перечисленных в ч. 3.3 настоящей статьи.

Чтобы минимизировать получение согласий на обработку различных массивов данных, организации следует разработать следующую внутреннюю документацию. Для противодействия информационным инцидентам необходимо разработать и принять локальные нормативные акты в организации, определяющие: 1) объем данных, обрабатываемых работодателем для противодействия информационным инцидентам; 2) лицо, ответственное за организацию обработки персональных данных; 3) перечень лиц, уполномоченных на внедрение противодействующих мер и осуществление внутренних расследований инцидентов информационной безопасности (вместе с должностными инструкциями и положениями об отделе; 4) процесс использования средств коммуникации для рабочих задач, включая ограничения и запреты на использование служебных средств коммуникации для личных целей; 5) право ответственного лица на доступ к информации, содержащейся в источниках рабочей коммуникации и порядок доступа; 6) полномочия ответственного лица и отдела информационной безопасности в организации в рамках противодействия инцидентам информационной безопасности; 7) использование антивирусных программ и иных программ, направленных на установление подозрительной активности; 8) порядок уничтожения данных работников в случае сбора лишних данных либо по достижении цели обработки данных. Работники должны быть ознакомлены с данными документами под роспись.

Указанные положения могут содержаться в документах с различными наименованиями. На практике их помещают в документы под названием «Политика информационной безопасности», «Регламент по реагированию на инциденты информационной безопасности», «Политика антивирусной защиты», «Положение об отделе информационной безопасности», «Регламент реагирования на инциденты информационной безопасности», «Политика использования собственных устройств в организации», «Политика конфиденциальности», «Положение о защите данных сотрудников» и др.

При определении объема обрабатываемых данных для принятия превентивных мер и проведения расследования необходимо соотносить обрабатываемые данные с целью противодействия инцидентам информационной безопасности. Если данные не являются необходимыми для достижения данной цели, тогда их обработка должна быть исключена, что вытекает из принципа минимизации обработки персональных данных, установленного в п. 4 ст. 5 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных». Например, в этой связи можно прийти к выводу, что обработка специальных категорий персональных данных (касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни) никоим образом не поможет расследованию инцидента информационной безопасности. Кроме того, при определении каналов и средств для рабочей коммуникации рекомендуется использовать рабочую почту, корпоративные мессенджеры и служебные технические средства, иначе риск сбора чрезмерного количества данных при проведении расследования повышается. Таким образом, используя перечисленные требования, в организации определяются категории информации, разрешенные для сбора, а также правомерность сбора необходимой информации специалистами и ответственность за нарушение законодательства при сборе.

Использование личных технических средств, осуществление рабочей коммуникации в мессенджерах типа Telegram или WhatsApp, где хранится как личная, так и служебная информация, затрудняют проведение полноценного законного расследования, так как данные источники в большинстве случаев содержат большое количество личной информации. Помимо общего ограничения, установленного принципом минимизации данных для конкретных целей, Трудовой кодекс Российской Федерации содержит положение, согласно которому работники не должны отказываться от своих прав на сохранение и защиту данных.

На настоящий момент отсутствует достаточное количество судебных дел, в рамках которых было рассмотрено данное положение, позволяющее утверждать об устоявшейся позиции судов, касающейся пределов ограничения права на защиту в рамках режимов тайн, применимых к рассматриваемой ситуации. В этой связи можно сделать вывод о том, что данный вопрос находится в области «полутени» («penumbra», «core and penumbra») права в терминологии Г. Харта. Очевидно, что даже при предоставленном согласии работника, постоянный контроль за его личной почтой, переписками в мессенджерах, смс-сообщениях является несоразмерным вторжением в сферу частной жизни работника. Как было отмечено в одном из судебных решений «работодатель не может требовать от работника предоставления персональных сведений, которые не связаны с осуществлением его трудовой деятельности в конкретной организации». В такой ситуации даже полученное согласие субъекта не защищает работодателя от ответственности за чрезмерное вторжение в частную жизнь работника. Это же относится и к иным основаниям обработки персональных данных. Например, в одном из судебных дел было указано, что даже при уведомлении сотрудников, установка камер видеонаблюдения работодателем в зоне отдыха не соответствует допустимым трудовым законодательством целям.

Но это же не означает, что частичное извлечение информации из данных источников, в соответствии с заявленными целями и в соответствующих объемах, обязательно должно расцениваться в качестве правонарушения, ведь иначе потребуется, чтобы каждый работодатель на территории Российской Федерации обеспечивал своих сотрудников личной

техникой, инфраструктурой (компьютеры, ноутбуки, телефоны) и каналами деловой связи для эффективного противодействия инцидентам информационной безопасности.

В этой связи разумно допустить, что использование данных источников в рамках противодействия инцидентам информационной безопасности может осуществляться на основании согласия работника, в котором будет указано, что работник разрешает работодателю извлекать информацию из данных источников в ситуации, когда инцидент информационной безопасности уже произошел и у работодателя наличествуют обоснованные основания полагать, что у в данных источниках может содержаться необходимая информация или в порядке добровольного предоставления сведений в рамках конкретных чатов. При непреднамеренном сборе чрезмерной информации работодатель обязан обеспечить немедленное уничтожение данной информации.

Однако для того, чтобы корректно собрать все минимально необходимые и допустимые для сбора с точки зрения законодательства данные, следует использовать специализированное программное обеспечение. Такое программное обеспечение необходимо использовать не только для самого процесса расследования, но и для хранения тех самых данных, необходимых для этого процесса. Данная необходимость связана с проблематикой корректного сбора, описанного в гл. 3 данной статьи. Если в организации не используются специализированные программные средства для хранения и резервирования данных, часто невозможно собрать даже минимальный набор необходимой для расследования информации. Также, только при использовании программного обеспечения для хранения, объём необходимых для сбора данных может не позволить быстро и корректно их собрать неавтоматизированным способом – данные уже могут быть неактуальны или модифицированы тем же злоумышленником. Тем самым вызвана необходимость использования специализированного программного обеспечения не только для сбора, но и для предварительного хранения и резервирования.

Также для выполнения требования законодательства в области уведомления компетентных органов необходимо осуществлять взаимодействие с правоохранительными и контролирующими органами. Данное взаимодействие предусматривает уведомление контролирующих органов об определенных инцидентах, а также при составе административного или уголовного правонарушения, взаимодействие с правоохранительными органами и судебными инстанциями. Выполнение перечисленных требований к уведомлению и отчетным мероприятиям об инцидентах регламентируется как для субъектов критической информационной инфраструктуры, так и для иных организаций, при расследовании инцидента, затронувшего персональные данных, обрабатываемые в организации.

В рамках внутренних расследований в российских организациях может возникнуть проблема наличия квалифицированных в данной области специалистов. Необходимость наличия профессиональных работников организации в сфере форензики заключается в сложности и комплексности процесса. Сложность заключается в необходимости использования различного программного обеспечения на разных этапах расследования. Комплексность заключается в применении не только технических, но и юридических знаний. Таким образом, специалисты должны обладать не только техническими навыками, но и быть специалистом в юридической сфере в части правомерного хранения, обработки и предоставления информации, присутствующей в системах организации, которые были представлены в четвертом разделе статьи.

Тем не менее, даже если специалист по информационной безопасности в организации владеет необходимыми юридическими основами, а также умеет использовать специализированное программное обеспечение, используемое для внутреннего расследования, могут получиться некорректные результаты без использования научно-технических решений в области форензики. Научно-технические решения могут состоять из различных подходов, методов, алгоритмов и методик, которые регламентируют совокупности и последовательность действий специалистов. К тому же научно-технические

решения могут быть как обобщенные, помогающие определить концептуальные моменты и этапы расследования, так и частные, которые могут конкретизировать действия сотрудников, относительно особенностей технического взаимодействия, использования специализированного программного обеспечения и корректной фиксации цифровых доказательств.

Таким образом, методика корректного расследования с технической и юридической точек зрения должна учитывать следующие требования к ее разработке:

1. Наличие внутренней документации, регламентирующей процессы проведения расследования, а также смежные с ними процессы.

2. Правила использования специализированного программного обеспечения, которое позволяет правильно хранить, собирать, извлекать, анализировать и представлять информацию, необходимую для расследования.

3. Наличие взаимодействия с контролирующими, правоохранительными и иными внешними органами во время и по результатам расследования.

4. Необходимость использования для расследования квалифицированных специалистов в данной области как с технической, так и с юридической точки зрения.

5. Необходимость использования для расследования научно-технических решений, которые позволяют построить процесс расследования.

С учётом быстроразвивающихся подходов как к реализации злоумышленниками преступных действий, так и к процессу проведения внутренних расследований в Российских организациях предложенные требования могут быть скорректированы или расширены.

Разработанные требования учитывают как юридические, так и технические проблемы существующих решений в области расследования внутренних инцидентов, которые были рассмотрены в данной статье.

Заключение

Несмотря на очевидные ограничения к сбору необходимой для расследования информации с юридической точки зрения, исполнение нормативно-правовых актов в области информационной безопасности, касающихся процесса внутреннего расследования, является не только обязательным для исполнения, но и позволяет выходить за рамки внутреннего расследования, при предоставлении результатов в контролирующих, правоохранительных и иных органах.

В статье были определены основные требования к методике расследования внутренних инцидентов, которая корректна как с технической, так и с юридической точки зрения. Разработанные требования были основаны на определенных в результате анализа релевантных работ проблемах, которые затрагивают как технические, так и юридические аспекты процесса. Синтез юридических и технических решений в обозначенной области позволит оптимизировать действия специалистов по расследованию инцидентов информационной безопасности, а также сформировать научную основу в данном направлении, относительно которой можно будет строить различные частные криминалистические решения, а также различные рекомендации по построению исследуемого процесса. Рекомендации могут быть применены для анализа существующих процессов проведения внутренних расследований в организациях и для разработки необходимой соответствующей документации в данной области.

Разработанная на основе определенных в статье рекомендаций методика внутреннего расследования, которая будет представлена во второй статье из цикла, сможет учесть все технические и юридические ограничения к данному процессу. К тому же данная методика будет применена для анализа уже проведенных расследований в российских организаций, с целью выявления некорректности проведения расследования с точки зрения разработанного междисциплинарного результата.

Список источников

1. Шаталов А.С. Феноменология преступлений, совершенных с использованием современных информационных технологий // Право. Журнал Высшей школы экономики. 2018. № 2. С. 68–83. DOI: 10.17323/2072-8166.2018.2.68.83.

2. Вершицкая Г.В. Возможности использования виртуальных следов в ходе расследования киберпреступлений // Вестник ПАГС. 2022. № 2. С. 17–23.

3. Лантух Э.В., Ишигеев В.С., Грибунов О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Всероссийский криминологический журнал. 2020. № 6. С. 882–890.

4. Решняк О.А. Современные способы совершения преступлений с использованием IT-технологий и проблемы расследования // Вестник Волгоградской академии МВД России. 2023. № 1 (64). С. 94–100.

5. Холевчук А.Г., Савченко А.В. Проблемы использования цифровых средств доказывания при расследовании преступлений в сфере компьютерной информации // Вестник ННГУ. 2021. № 5. С. 149–154.

6. Шушеначев А.В. Правовое регулирование сбора цифровой информации с целью ее представления как доказательства в расследовании преступлений // Юридическая наука. 2023. № 1. С. 122–126.

7. Горда М.Д., Чечулин А.А. Модель расследования киберпреступлений // информатизация и связь. 2023. № 3. С. 92–97. DOI: 10.34219/2078-8320-2023-14-3-92-97.

8. Chechulin A., Gorda M. Cybercrime Investigation Model // 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2024. P. 37–42. DOI: 10.1109/COMSNETS59351.2024.10427215.

9. Вершицкая Г.В. Возможности использования виртуальных следов в ходе расследования киберпреступлений // Вестник ПАГС. 2022. № 2. С. 17–23. DOI: 10.22394/1682-2358-2022-2-17-23.

10. Desnitsky V., Kotenko I., Chechulin A. Configuration-based approach to embedded device security. Lecture Notes in Computer Science, Springer-Verlag // Lecture Notes in Computer Science. 2012. Iss. 7531 LNCS. P. 270–285.

11. Алиев Т.Ф. Вопросы противодействия преступлениям, совершаемым с использованием IT-технологий // Юридические исследования. 2023. № 10. С. 100–114. DOI: 10.25136/2409-7136.2023.10.44173.

References

1. Shatalov A.S. Fenomenologiya prestuplenij, sovershennyh s ispol'zovaniem sovremennyh informacionnyh tekhnologij // Pravo. Zhurnal Vysshej shkoly ekonomiki. 2018. № 2. S. 68–83. DOI: 10.17323/2072-8166.2018.2.68.83.

2. Vershickaya G.V. Vozmozhnosti ispol'zovaniya virtual'nyh sledov v hode rassledovaniya kiberprestuplenij // Vestnik PAGS. 2022. № 2. S. 17–23.

3. Lantuh E.V., Ishigeev V.S., Gribunov O.P. Ispol'zovanie special'nyh znanij pri rassledovanii prestuplenij v sfere komp'yuternoj informacii // Vserossijskij kriminologicheskij zhurnal. 2020. № 6. S. 882–890.

4. Reshnyak O.A. Sovremennye sposoby soversheniya prestuplenij s ispol'zovaniem IT-tekhnologij i problemy rassledovaniya // Vestnik Volgogradskoj akademii MVD Rossii. 2023. № 1 (64). S. 94–100.

5. Holevchuk A.G., Savchenko A.V. Problemy ispol'zovaniya cifrovyh sredstv dokazyvaniya pri rassledovanii prestuplenij v sfere komp'yuternoj informacii // Vestnik NNGU. 2021. № 5. S. 149–154.

6. Shushenachev A.V. Pravovoe regulirovanie sbora cifrovoj informacii s cel'yu ee predstavleniya kak dokazatel'stva v rassledovanii prestuplenij // Yuridicheskaya nauka. 2023. № 1. S. 122–126.

7. Gorda M.D., Chechulin A.A. Model' rassledovaniya kiberprestuplenij // informatizaciya i svyaz'. 2023. № 3. S. 92–97. DOI: 10.34219/2078-8320-2023-14-3-92-97.

8. Chechulin A., Gorda M. Cybercrime Investigation Model // 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2024. P. 37–42. DOI: 10.1109/COMSNETS59351.2024.10427215.

9. Vershickaya G.V. Vozmozhnosti ispol'zovaniya virtual'nyh sledov v hode rassledovaniya kiberprestuplenij // Vestnik PAGS. 2022. № 2. S. 17–23. DOI: 10.22394/1682-2358-2022-2-17-23.

10. Desnitsky V., Kotenko I., Chechulin A. Configuration-based approach to embedded device security. Lecture Notes in Computer Science, Springer-Verlag // Lecture Notes in Computer Science. 2012. Iss. 7531 LNCS. P. 270–285.

11. Aliev T.F. Voprosy protivodejstviya prestupleniyam, sovershaemym s ispol'zovaniem IT-tekhnologij // Yuridicheskie issledovaniya. 2023. № 10. S. 100–114. DOI: 10.25136/2409-7136.2023.10.44173.

Информация о статье:
Статья поступила в редакцию: 08.09.2024; одобрена после рецензирования: 28.09.2024;
принята к публикации: 29.09.2024
Information about the article:
The article was submitted to the editorial office: 08.09.2024; approved after review: 28.09.2024;
accepted for publication: 29.09.2024

Сведения об авторах:
Чечулин Андрей Алексеевич, ведущий научный сотрудник Санкт-Петербургского федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14 линия В.О., д. 39), кандидат технических наук, доцент, e-mail: andreych@bk.ru, https://orcid.org/0000-0001-7056-6972
Горда Максим Дмитриевич, младший научный сотрудник Санкт-Петербургского федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14 линия В.О., д. 39), e-mail: gordamd@yandex.ru, https://orcid.org/0009-0009-1301-7294, SPIN-код: 3530-7860
Котов Александр Александрович, аспирант Санкт-Петербургского федерального исследовательского центра Российской академии наук (199178, Санкт-Петербург, 14 линия В.О., д. 39), e-mail: alexanderkotovspb@gmail.com, https://orcid.org/0000-0002-7718-5256, SPIN-код: 6153-5820

Information about the authors:
Chechulin Andrey A., leading researcher at the Saint-Petersburg federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14 line V.O., 39), candidate of technical sciences, associate professor, e-mail: andreych@bk.ru, https://orcid.org/0000-0001-7056-6972
Gorda Maxim D., junior researcher at the Saint-Petersburg federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14 line V.O., 39), e-mail: gordamd@yandex.ru, https://orcid.org/0009-0009-1301-7294, SPIN: 3530-7860
Kotov Alexander A., postgraduate student at the Saint-Petersburg federal research center of the Russian academy of sciences (199178, Saint-Petersburg, 14 line V.O., 39), e-mail: alexanderkotovspb@gmail.com, https://orcid.org/0000-0002-7718-5256, SPIN: 6153-5820