Научная статья
УДК 347.21, 347.775
DOI: https://doi.org/10.17323/tis.2022.14227

Original article

К ВОПРОСУ ОБ ОХРАНЕ КОММЕРЧЕСКОЙ ТАЙНЫ НА ПРЕДПРИЯТИЯХ АДДИТИВНОГО ПРОИЗВОДСТВА В УСЛОВИЯХ НЕОБХОДИМОСТИ УДАЛЕННОГО ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ КОМПАНИИ

TO THE QUESTION OF PROTECTION OF TRADE SECRETS AT ADDITIVE MANUFACTURING ENTERPRISES IN THE CONTEXT OF THE REQUIREMENT FOR REMOTE INTERACTION OF THE COMPANY'S DEPARTMENTS

Владислав Валерьевич СОМОНОВ
Санкт-Петербургский государственный университет информационных технологий, механики и оптики, Санкт-Петербург, Россия,
vlad@ltc.ru,
https://orcid.org/0000-0002-4962-9411

Ксения Романовна КОЛОМОЙЦЕВА
Санкт-Петербургский государственный университет информационных технологий, механики и оптики, Санкт-Петербург, Россия,
Ksenchik97@yandex.ru,
https://orcid.org/0000-0002-1894-2632

Владимир Сергеевич КОЛОМОЙЦЕВ
Санкт-Петербургский университет аэрокосмического приборостроения, Санкт-Петербург, Россия,
Dekoros@guap.ru,
https://orcid.org/0000-0001-7282-033X

Информация об авторе
В.В. Сомонов — магистрант факультета технологического менеджмента и инноваций Санкт-Петербургского государственного университета информационных технологий, механики и оптики
К.Р. Коломойцева — магистрант факультета технологического менеджмента и инноваций Санкт-Петербургского государственного университета информационных технологий, механики и оптики
В.С. Коломойцев — кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского университета аэрокосмического приборостроения

Аннотация. Новая короновирусная инфекция оказала сильное влияние на мировую экономику, что привело к некоторым изменениям при работе с объектами интеллектуальной собственности. При данных обстоятельствах приходится быстро адаптироваться к новому режиму работы всему миру, в том числе и компаниям, работающим в сфере аддитивного производства, в которых постоянно появляются новые объекты интеллектуальной собственности. Изменились привычные способы работы не только государственных ведомств, занимающихся интеллектуальной собственностью, но и частных компаний, использующих ее в своей работе. Работа в удаленном режиме влечет за собой ряд особенностей, несоблюдение которых может привести к нежелательным последствиям для компаний. Для новых условий осуществления деятельности необходимы новые способы охраны объектов интеллектуальной собственности.

Работа посвящена изучению проблемы охраны коммерческой тайны в условиях экономического кризиса, вызванного новой коронавирусной инфекцией. Сформулированы группы методов по защите конфиденциальной информации, составляющей коммерческую тайну: методы, обеспечивающие работу с документами; организационные методы; информационно-аналитические методы. Показаны основные причины и каналы утечки конфиденциальной информации. Основными причинами утечки информации являются непривилегированные

сотрудники, а основным каналом — использование для передачи информации, содержащей коммерческую тайну, программ для общения в интернете (мессенджеров) или незащищенных каналов передачи информации о параметрах технологии 3D-печати и оборудовании для нее.

Рассмотрены особенности защиты коммерческой тайны при удаленном режиме работы. Разработаны меры предотвращения распространения конфиденциальной информации, позволяющие минимизировать вероятность наступления нежелательных последствий и предотвратить финансовые потери компаний. Предложены способы защиты коммерческой тайны в условиях организации удаленного доступа к ресурсам компании: обеспечение высокого уровня защищенности персональных данных сотрудников; присутствие в компании специалиста по информационной безопасности; безопасная выделенная линия связи в интернете.

Ключевые слова: аддитивное производство, коммерческая тайна, конфиденциальная информация, несанкционированный доступ, интеллектуальная собственность, защита информации, удаленный доступ, утечка информации, персональные данные

Для цитирования: *Сомонов В.В., Коломойцева К.Р., Коломойцев В.С.* К вопросу об охране коммерческой тайны на предприятиях аддитивного производства в условиях необходимости удаленного взаимодействия подразделений компании // Труды по интеллектуальной собственности (Works on Intellectual Property). 2022. Т. 40, № 1. С. 118–126;
DOI: https://doi.org/10.17323/tis.2022.14227

Vladislav V. SOMONOV
Saint Petersburg State University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia,
vlad@ltc.ru,
https://orcid.org/0000-0002-4962-9411

Ksenia R. KOLOMOYTSEVA
Saint Petersburg State University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia,
Ksenchik97@yandex.ru,
https://orcid.org/0000-0002-1894-2632

Vladimir S. KOLOMOITCEV
State University of Aerospace Instrumentation,
St. Petersburg, Russia,
dekoros@guap.ru,
https://orcid.org/0000-0001-7282-033X

Information about the author
V.V. Somonov — student of the Faculty of Technological Management and Innovation of Saint Petersburg State University of Information Technologies, Mechanics and Optics
K.R. Kolomoytseva — student of the Faculty of Technological Management and Innovation of Saint Petersburg State University of Information Technologies, Mechanics and Optics
V.S. Kolomoitcev — PhD in engineering, Associate Professor of the Department No 51. Information Systems Security, State University of Aerospace Instrumentation

Abstract. The new coronavirus infection has a strong impact on the global economy. This led to some changes when working with intellectual property. Under these circumstances, the whole world has to adapt quickly to the new mode of operation, including companies working in the field of additive manufacturing. The new intellectual property objects are constantly appearing in these companies. It is changed the ways not only government agencies dealing with intellectual property work, but also private companies that use it in their work. Failure to comply with a number of features may lead to undesirable consequences for companies when working remotely. For new conditions for the implementation of activities, new ways of protecting intellectual property objects are required.

The paper is devoted to the study of the problem of protecting trade secrets in the context of the economic crisis caused by a new coronavirus infection. The groups of methods for the protection of confidential information constituting a trade secret are formulated: methods that ensure the work with documents; organizational methods; information and analytical methods. The main reasons and ways of confidential information leakage are shown. Unprivileged employees are the main causes of information leakage and the main path of information leakage is the use of programs for communication on the Internet (instant messengers) or unprotected channels for transmitting information about the parameters of 3D printing technology and equipment for it to transmit information containing trade secrets. The features of protection of trade secrets during remote operation are considered. The ways to prevent the dissemination of confidential information are developed. They will minimize the probability of undesirable consequences and prevent financial losses for companies. Methods of protecting trade secrets in the context of organizing remote access to company resources are proposed: ensure a high level of protection of personal data of employees; presence of an information security specialist in the company; secure dedicated communication line in the Internet.

Keywords: additive manufacturing; trade secret; confidential information; unauthorized access; intellectual property; protection of information; remote access; information leak; personal data

For citation: *Somonov V.V., Kolomoitseva K.V., Kolomoitsev V.S.* On the issue of the problem of protecting trade secrets at additive manufacturing enterprises in the context of the need for remote interaction of company divisions // Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property). 2022. Vol. 40 (1). P. 118–126;
DOI: https://doi.org/10.17323/tis.2022.14227

Современное общество находится на стадии четвертой промышленной революции (Индустрия 4.0), что способствует активному накоплению больших данных и внедрению интеллектуальных производственных систем и передовых информационных технологий. Одним из видов таких технологий по заявлению авторов работы [10] является аддитивное производство. Успешная обработка и анализ этих данных при таком виде производства [12] предоставляют новые возможности для компаний. С.Л. Добрынин и В.Л. Бурковский [3] отметили тот факт, что традиционно в подобных компаниях производственные данные собираются от оборудования, установленного в цехах, затем они транслируются благодаря технологии интернета вещей до хранилищ информации. Все это повышает эффективность производства. При этом обеспечивается массовая индивидуализация за счет использования нетрадиционных методов производства [9].

С другой стороны, имеющаяся у компаний в этой сфере важная и потенциально коммерчески выгодная информация должна охраняться соответствующим образом. Коммерческая тайна, согласно Федеральному закону от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 09.03.2021), — это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [8].

Актуальность настоящего исследования связана со стремительными изменениями, происходящими во всем мире, вызванными новой коронавирусной инфекцией. Организация работы удаленно влечет за собой необходимость усиления охраны коммерческой тайны и создания новых критериев ее существования. Вопросы обеспечения сохранности конфиденциальной информации исследовались и до наступления экономического кризиса такими авторами, как Н.Д. Попов, В.В. Колесник, Д.В. Головкина, Е.К. Волчинская, Д.С. Мащенко и др. [1, 2, 5, 6]. Сегодня же из-за недавности событий данная тема недостаточно хорошо научно разработана, что еще раз подтверждает ее актуальность.

Таким образом, необходима разработка (или усовершенствование существующих) эффективных мер и методов предотвращения или снижения вероятности распространения конфиденциальной информации, содержащей коммерческую тайну, на предприятиях, работающих в сфере аддитивного производства.

Информация, составляющая коммерческую тайну, может быть представлена сведениями различного характера: производственного, технического, экономического, организационного и других [2]. Традиционно в компаниях из сферы аддитивного производства каждый менеджер помимо владения своими персональными данными имеет доступ к информации, составляющей секрет производства или являющейся потенциально коммерчески выгодной. Она относится как к его собственному иерархическому уровню, так и ко всем нижестоящим уровням. Не каждый менеджер компании заинтересован в том, чтобы доплачивать своим подчиненным за обеспечение поддержания режима коммерческой тайны [14]. Это приводит к необходимости выстраивания и внедрения специальной системы для защиты коммерческой тайны.

Методы защиты коммерческой тайны можно разбить на три группы:

- методы, обеспечивающие работу с документами. Они включают в себя правила распространения документов, содержащих конфиденциальную информацию;
- организационные методы, которые включают в себя три способа защиты коммерческой тайны: установление корпоративных правил коммерческой конфиденциальности; определение порядка взаимодействия сотрудников; организационно-структурную изоляцию, позволяющую обеспечить доступ к коммерческой тайне только сотрудникам, работающим с ней;
- информационно-аналитические методы, которые представляют собой способы, позволяющие предотвратить утечку информации по причине принадлежности ее к коммерческой тайне [6].

В России в 2020 г. число утечек информации, составляющей коммерческую тайну, выросло на 5,6% по сравнению с аналогичным периодом прошлого года [7]. Доля утечек по вине сотрудников вдвое выше, чем в мире, — более 72%. Свыше 79% утечек произошло в результате внутренних нарушений — из них по вине непривилегированных сотрудников 72,1% и 5% по вине руководителя [7].

Приведенные статистические данные показывают, что необходимо разработать набор методов, правил и мер, позволяющих повысить безопасность при работе с информацией, содержащей коммерческую тайну. Так, следует ознакомить каждого сотрудника организации с правилами и режимом работы с конфиденциальной информацией, в том числе с режимом коммерческой тайны [11]. В период удаленной работы доступ к коммерческой тайне по ошибке может получить сотрудник, не допущенный к ней по существующим правилам разграничения доступа. В результате, не зная особенностей работы с подобной информацией, такой сотрудник может по ошибке (по незнанию) или целенаправленно осуществить ее разглашение, в том числе и на официальных мероприятиях.

Как во всем мире, так и в России более 80% случаев утечки конфиденциальной информации связаны с раскрытием персональных данных. Высокая доля утечек коммерческой тайны связана с критически важным значением этого типа информации для многих компаний [7]. На рис. 1 представлено распределение утечек по типам данных [7].

В аддитивном производстве под конфиденциальной информацией, составляющей коммерческую тайну или охраняющейся в режиме ноу-хау, обычно понимают параметры режима 3D-печати и постобработки изделий, настройки или особенности оборудования, необходимого для реализации процессов, а также требования к подготовке либо анализу химического или

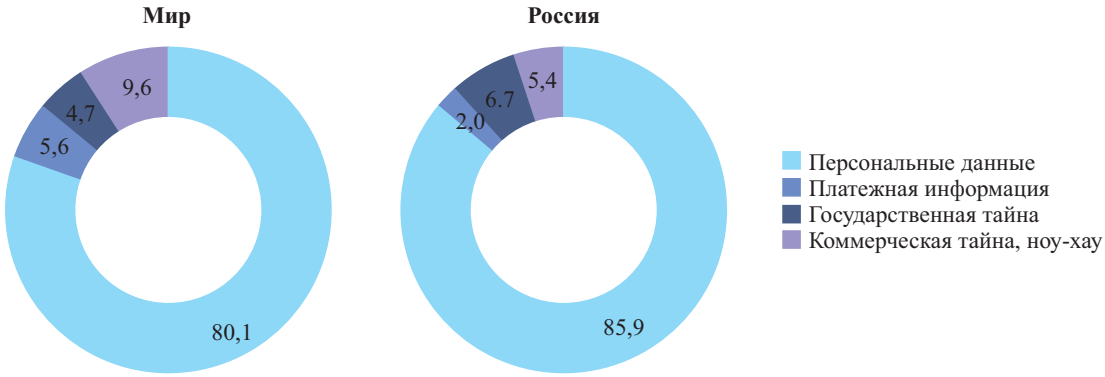

Рисунок 1. Распределение утечек по типам данных в России и в мире, январь — сентябрь 2020 г.

структурного состава материалов для изготовления изделий таким методом.

Из рис. 1 видно, что утечки информации в этой области в последнее время увеличились вместе с ростом популярности аддитивных технологий и составляют существенную долю. Это заставляет компании серьезно задумываться о сохранении секрета своих разработок и защите их от конкурентов. Они также могут патентовать разработки, но в дальнейшем возникает проблема прекращения правовой охраны и перехода в общественное достояние. Такое развитие событий компаниям крайне невыгодно, поэтому они часто патентуют свои разработки без указания точных значений параметров режима процесса 3D-печати изделий из конкретных материалов, а остальное охраняют в режиме ноу-хау.

Зачастую несанкционированный доступ к коммерческой тайне можно получить и благодаря персональным данным сотрудников, имея доступ к их аккаунтам или иным образом [1, 4]. Используя эти данные, можно через аккаунт сотрудника выяснить техническую и другую информацию на его уровне доступа. В связи с этим для защиты коммерческой тайны в период работы организации удаленно важно обеспечивать сохранность персональных данных своих сотрудников и предотвращать несанкционированный доступ к ним.

Основным каналом утечки конфиденциальной информации выступает интернет. На рис. 2 представлено распределение утечек по каналам передачи информации [7].

Из представленных данных следует, что необходимо предпринять серьезные усилия по повышению информационной защищенности коммерческой тайны, используемой компаниями из области аддитивного производства в сети и облачных хранилищах. Ведь она может представлять собой данные поставщиков материалов для 3D-печати, рабочие 3D-модели для построения изделий, информацию по процессу построения, о настройках оборудования, о защитной атмосфере в ходе реализации процесса построения изделия, о режимах постобработки и выдержки изделий, а также о результатах испытаний после получения готового изделия и другую важную информацию, представляющую интерес для конкурентов.

Традиционно в сфере аддитивного производства новые данные, представляющие коммерческую ценность и требующие охраны, получают в рамках выполнения НИР или НИОКР. Для того чтобы в дальнейшем найти им выгодное применение и чтобы они не утекли к конкурентам, необходимо пройти несколько стадий до введения на предприятии режима коммерческой тайны, позволяющего сохранять данные в секрете до момента передачи по лицензии или продажи заинтересованному покупателю. Создаваемые в рамках НИР 3D-модель и чертежи будущей выращиваемой заготовки должны регистрироваться в базе данных организации. А при разработке в рамках НИОКР-комплексов вся конструкторская и технологическая документация должна засекречиваться до момента принятия руководством решения о режиме правовой охраны. После этого должна разрабатываться техническая документация, содержащая важные данные о процессе выращивания заготовки на конкретном комплексе.

На следующем этапе разработчики уведомляют патентно-лицензионную службу или специалистов по интеллектуальной собственности в организации о разработке документов, содержащих данные, представляющие коммерческую ценность, а те, в свою очередь, регистрируют это в журнале учета уведомлений и подписывают с ними соглашение о неразглашении. Затем сотрудники патентно-лицензионной службы доносят эту информацию до руководства, которое

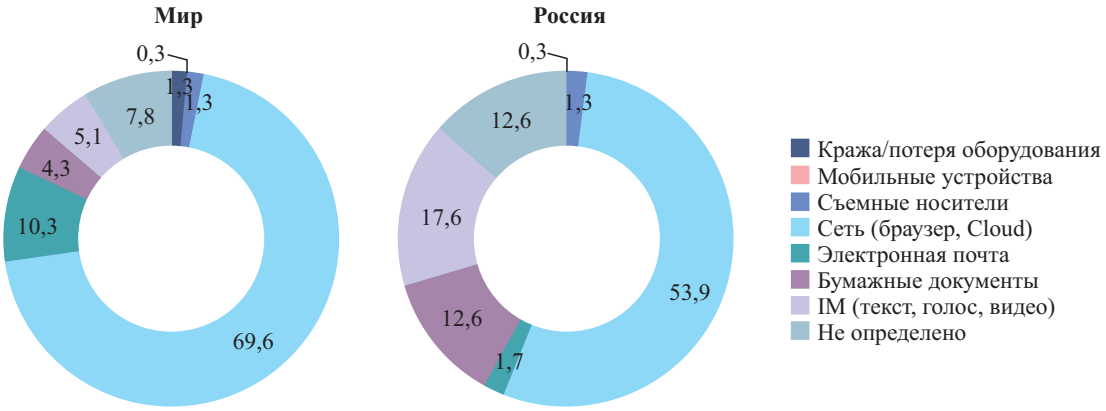

Рисунок 2. Распределение утечек по каналам передачи информации в России и в мире, январь — сентябрь 2020 г.

с учетом стратегии развития организации и политики по управлению интеллектуальной собственностью принимает решение о том, какие из представленных данных необходимо охранять в режиме коммерческой тайны, а какие стоит патентовать. После выбора конкретных данных и режима охраны вводится режим коммерческой тайны. Он оформляется в виде приказа по организации, формируется перечень лиц, имеющих доступ к секретной информации, и определяется способ ее хранения, в том числе и на электронных носителях.

Далее на протяжении всего цикла получения дохода от охраняемых коммерческой тайной сведений необходимо осуществлять управление рисками:

1. Осуществлять меры по предотвращению утечек конфиденциальных сведений и иных нарушений установленного режима коммерческой тайны или конфиденциальности.

Каждый шестой случай компрометации конфиденциальных данных в России происходит через программы для общения в интернете (мессенджеры) [7]. В России, как и во всем мире, активно их используют для быстрой передачи недавно полученных результатов разработок, например результатов экспериментов по отработке каких-либо стратегий построения изделий. В связи с этим компании, работающей удаленно и использующей в качестве канала связи интернет, сложно избежать утечки информации.

Для того чтобы режим коммерческой тайны стабильно функционировал, необходимо осуществлять периодический контроль со стороны назначенного ответственного лица соблюдения всех установленных условий конфиденциальности лицами, имеющими доступ к охраняемым сведениям. Также компаниям следует периодически проверять те меры, которые были предприняты для сохранности выбранных сведений. Это поможет контролировать, насколько эффективно и своевременно они применяются, и, если требуется, корректировать их.

Поэтому руководителям компаний, работающих в области 3D-печати, важно обеспокоиться внедрением способа взаимодействия и связи с сотрудниками для передачи конфиденциальной информации о технологии, оборудовании для 3D-печати, о поставщиках материалов и др. В качестве такого сервиса может выступить собственный сервер компании или выделенная безопасная линия связи, реализованная, например, посредством VPN-технологии [13].

При построении системы безопасной охраны в цифровом пространстве создаваемых коммерчески выгодных данных следует руководствоваться следующими рекомендациями:

- она должна иметь простую архитектуру, состоять из простых компонентов, иметь минимально возможное число каналов и протоколов межсетевого взаимодействия. В системе должны присутствовать только те элементы, которые нужны ей для работы;
- рабочий процесс компании должны внедрять только предварительно протестированные программные решения, у которых известны все их преимущества и недостатки;
- в случае необходимости в них могут вноситься минимальные доработки силами сотрудников компании или привлеченных исполнителей, но без разглашения информации о тонкостях архитектуры программного решения и принципов его действия;
- компаниям следует применять только лицензированное ПО, по возможности оно должно быть внесено в государственный реестр программ для ЭВМ и баз данных; это позволит в дальнейшем понимать, к кому предъявлять претензии в случае некорректной работы;
- при создании системы стоит применять только аутентичные компоненты как долговечные и более надежные, что позволит всей системе не выходить неожиданно из строя. Должна учитываться совместимость всех компонентов;
- необходимо иметь возможность управлять как создаваемой системой целиком, так и отдельными программами или компонентами, пользуясь для этого минимальным количеством обращений к сторонней технической поддержке;
- в момент выявления факта утечки информации, обладающей коммерческой ценностью, компания должна предпринять попытку ее локализации. После этого необходимо определить источник, откуда она передается посторонним лицам, а также выяснить, куда она передается.

В компании должно быть организовано протоколирование и документирование любых действий сотрудников, работающих с охраняемой информацией, хранящейся в виде файлов, а также протоколирование и документирование случаев несанкционированного доступа к данным. Защита охраняемых данных должна быть многоуровневой. Каждый потенциальный канал утечки должен охраняться на нескольких уровнях. Это затруднит потенциальному похитителю доступ к охраняемым сведениям компании.

Для решения таких задач в штате компании, занимающейся аддитивным производством, должны быть сотрудники, имеющие определенные компетенции, позволяющие им предпринять все необходимые меры. Наличие в компании специалиста по информационной безопасности также позволяет повысить степень обоснованности принимаемых решений при проек-

тировании системы защиты информации, обеспечивающей защиту коммерческой тайны информации, обрабатываемой в информационной системе компании [4], с тем чтобы заранее определять слабые места в существующей системе и попытаться их усилить или устранить при обновлении структуры системы. Качественно спроектированная и построенная система защиты информации снижает риск возможной ее утечки и в результате, повышает эффективность работы компании. Таким образом, возникает необходимость расширить кадровый состав и нанять специалиста (или нескольких специалистов) по информационной безопасности либо, в случае невозможности принятия данного решения, воспользоваться помощью компаний, специализирующихся в области оказания услуг по построению защищенных инфокоммуникационных систем.

Хорошим решением также может стать приглашение сертифицированных в области информационной безопасности аудиторских компаний для получения объективной оценки состояния информационной защищенности компании и выработки индивидуальных решений по построению эффективной как с точки зрения безопасности, так и с точки зрения производительности системы с учетом всех бизнес-процессов в компании.

Для повышения сохранности сведений необходимо уменьшить доступ к конфиденциальным сведениям.

Компания должна создать свою локальную сеть, в которую будут выводиться по защищенным каналам для хранения охраняемые данные. При организации доступа к таким данным должны использоваться технические средства ограничения обмена данными с внешней средой (устройства для криптографической защиты, осуществляющие шифрование данных на рабочих станциях, комплексах для выращивания и серверах компании, передаваемых по каналам связи; различные средства антивирусной защиты; SIEM-системы и DLP-системы, обеспечивающие закрытие всех потенциальных каналов утечки информации и перехват исходящего трафика; сетевые фильтры, файерволы, устройства для контроля доступа к серверам; физическая защита средств коммутации с использованием специальных замков или блокировок). Помимо технических средств должны быть внедрены организационные меры (ограничения на использование сторонних носителей информации, на подключение сторонних устройств к терминалам доступа в локальную сеть, введение ограничений по внесению в места обеспечения доступа к локальной сети средств воспроизведения информации — смартфонов, камер и т.д).

Компаниям, работающим в сфере аддитивного производства, необходимо осуществлять поступательную модернизацию системы контроля конфиденциальности сведений по мере увеличения их объема, увеличения количества лиц, которые имеют доступ к сведениям и пользуются ими, усложнения производства. Это связано с тем, что у таких компаний в силу специфики передачи данных через каналы связи и из-за постоянного развития средств и алгоритмов для ее изъятия в цифровом пространстве должны быть адекватные средства противодействия возможным атакам со стороны конкурентов.

При создании параллельно сразу нескольких разных объектов для выращивания или при масштабном серийном производстве необходимо выполнять классификацию и дифференциацию создаваемых данных (охраняемых сведений) относительно каждого получаемого в результате работ сотрудников технического решения или способа осуществления их профессиональной деятельности. Они должны распределяться по различным местам хранения в системе (на сервере) или носителям. В определенных случаях даже можно установить различный режим доступа к конкретным частям данных для конкретных сотрудников компании. Это позволит предупредить одномоментную потерю конфиденциальности для всего массива сведений, усложнить конкурентам получение всей секретной информации через один источник утечки.

В качестве примера разделения такой информации можно привести следующий вариант. Сведения о процессе выращивания изделия в целом можно представить как сумму сведений на различных этапах производства, например сведения об этапе подготовки рабочего инструмента на этапе 1 +...+ сведения о постобработке выращенного изделия на этапе N.

Доступ к определенным сведениям, находящимся в том числе в памяти оборудования для аддитивного производства и на сервере для передачи и хранения уже созданных моделей, управляющих программ, результатов испытаний, должны иметь только конкретные лица (персонал), которым использование этих данных необходимо для осуществления соответствующих трудовых функций.

В процессе массового использования цифрового формата создания данных, которые представляют коммерческую ценность и должны охраняться в режиме коммерческой тайны, компаниям из сферы аддитивного производства просто необходимо внедрить у себя автоматизированную систему управления результатами интеллектуальной деятельности (РИД). Она поможет ускорить процесс учета создаваемой ценной информации, которую руководство решает сохранить в тайне. Это будет способствовать повышению эффективности управления системой для предотвращения утечек и снижению потерь создаваемых

технических решений из-за упрощения учета и управления возникающими в процессе деятельности компаний РИД. Наличие в этой автоматизированной системе реестра всех значимых событий, касающихся РИД, позволит в случае необходимости подтвердить свои права на созданные данные.

2. Требуется осуществлять мониторинг правовой чистоты полученной информации, которая охраняется коммерческой тайной.

Выбранный руководством компании массив сведений, который охраняется в режиме коммерческой тайны, ввиду специфики аддитивного производства и создания управляющих программ или моделей для выращивания может впоследствии пополняться новыми сведениями. В результате происходит трансформация охраняемой информации и ее юридического статуса. После добавления новых данных это уже обновленный массив, новое техническое решение, которое требует введения режима коммерческой тайны. Поэтому необходимо осуществлять систематический контроль того, не нарушает ли использование сформированного массива сведений исключительных прав какого-либо третьего лица. Если добавленные данные не являются итогом творчества сотрудников компании, которые не создали данные в результате выполнения задания работодателя в рабочее время, в рамках своей должностной инструкции и на мощностях компании, а взяли их из интернета или у сторонних лиц, то необходимо получить право использования этой информации в коммерческих целях у ее правообладателя путем заключения соответствующего договора.

Для высокоэффективной работы с коммерческой тайной компании в лице ее руководства необходимо уделять большое внимание следующему:

- решению вопроса о необходимости найма дополнительных сотрудников, в обязанности которых будут входить поддержание безопасной работы инфокоммуникационной системы компании, работающей в сфере аддитивного производства, и в случае необходимости ее модернизация;
- ознакомлению каждого сотрудника организации с правилами и режимом работы с конфиденциальной информацией;
- для предотвращения распространения конфиденциальной информации необходимо усилить защиту персональных данных сотрудников, что снизит вероятность несанкционированного доступа в систему от лица скомпрометированных сотрудников;
- исследованию и внедрению методов безопасного взаимодействия и связи с сотрудниками компании, а также передаче важных данных о процессах, материалах и оборудовании в области 3D-печати; такими методами могут быть выделенные серверы или выделенная безопасная линия связи.

Результаты, полученные в настоящем исследовании, позволяют повысить информационную защищенность компаний из сферы аддитивного производства и информационных систем, использующихся в них при обработке сведений, составляющих коммерческую тайну. Это, в свою очередь, дает возможность снизить риск финансовых потерь компаний. Направлениями дальнейших исследований могут стать рассмотрение и исследование специфических методов защиты информации и выработка способов сокращения расходов на защиту коммерческой тайны.

СПИСОК ИСТОЧНИКОВ

1. *Волчинская Е.К.* Место персональных данных в системе информации ограниченного доступа // Право. Журнал Высшей школы экономики. 2014. № 4. С. 193–207.
2. *Головкина Д.В.* Обеспечение информационной безопасности установлением режима коммерческой тайны // Вестник Прикамского социального института. 2019. № 1 (82). С. 12–16.
3. *Добрынин С.Л., Бурковский В.Л.* Проблематика управления аддитивным производством на основе технологий промышленного интернета вещей // Вестник Воронежского государственного технического университета. Т. 17. № 2. 2021, С. 7–13.
4. *Коломойцев В.С., Богатырев В.А.* Эффективность поэтапного применения средств защиты с пересечением областей обнаружения угроз // Программные продукты и системы. 2018. Т. 32. № 3. С. 557–564.
5. *Мащенко Д.С.* Концептуальные вопросы организации информационно-экономической безопасности // Вестник Самарского государственного аэрокосмического университета. 2004. № 2, С. 21–25.
6. *Попов Н.Д.* Способы защиты коммерческой тайны юридическими лицами // Правовая система России: история и современность: сборник статей Международной научно-практической конференции (23 декабря 2017 г., Екатеринбург). Уфа: Омега Сайнс, 2017. С. 190–193.
7. Утечки информации ограниченного доступа: отчет за девять месяцев 2020 г. [Электронный ресурс] // Экспертно-аналитический центр InfoWatch. 2020. 26 с.
8. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ // Российская газета — Федеральный выпуск № 0(3543). 05.08.2004.
9. *Despeisse M., Ford S.* The Role of Additive Manufacturing in Improving Resource Efficiency and Sustainability // Centre for Technology Management working paper series, 2015. No 3, 9 s.

10. *Dilberoglua U. M., Gharehpapagh B., Yaman U., Dolen M.* The role of additive manufacturing in the era of Industry 4.0 // Procedia Manufacturing. 2017. Vol. 11, S. 545–554.
11. *Kasdan Michael J., Smith Kevin M.* Daniels Benjamin Trade Secrets: What You Need to Know // The national law review — Wiggin and Dana LLP, 2019. Volume IX, № 346.
12. *Moshiria M., Charles A., Elkaseer Ah. e.a.* An Industry 4.0 framework for tooling production using metal additive manufacturing-based first-time-right smart manufacturing system // Procedia CIRP 93 (2020). S. 32–37.
13. *Nesteruk Ph., Kharchenko A., Nesteruk G.* Information safety in electronic business: adaptive model of systems safety of information technologies // Proc. of Int. Conf. "Information technology in business" (St. Petersburg, October 8–10, 2003). St. Petersburg, 2003. S. 124–128.
14. *Zabojnik J.* A theory of trade secrets in firms // International economic review. Vol. 43, Issue 3, 2002. S. 831–855.

REFERENCES

1. *Volchinskaya E.K.* Mesto personal'nyh dannyh v sisteme informacii ogranichennogo dostupa / Pravo. Journal of the Higher School of Economics. 2014. No 4. S. 193–207.
2. *Golovkina D.V.* Obespechenie informacionnoj bezopasnosti ustanovleniem rezhima kommercheskoj tajny // Vestnik Prikamskogo social'nogo instituta. No 1 (82). 2019. S. 12–16.
3. *Dobrynin S.L., Burkovskij V.L.* Problematika upravleniya additivnym proizvodstvom na osnove tekhnologij promyshlennogo interneta veshchej // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. T. 17. № 2. 2021, S. 7–13.
4. *Kolomoitsev V.S., Bogatyrev V.A.* Effektivnost' poetapnogo primeneniya sredstv zashchity s peresecheniem oblastej obnaruzheniya ugroz // Programmnye produkty i sistemy. 2018. T. 32. No 3. S. 557–564.
5. *Mashchenko D.S.* Konceptual'nye voprosy organizacii informacionno-ekonomicheskoj bezopasnosti // Vestnik Samarskogo gosudarstvennogo aerokosmicheskogo universiteta. 2004. No 2. S. 21–25.
6. *Popov N.D.* Sposoby zashchity kommercheskoj tajny yuridicheskimi licami // Pravovaya sistema Rossii: istoriya i sovremennost': sbornik statej Mezhdunarodnoj nauchno — prakticheskoj konferencii (23 dekabrya 2017 g, Ekaterinburg). Ufa: Omega Sajns. 2017. S. 190–193.
7. Utechki informacii ogranichennogo dostupa: otchet za 9 mesyacev 2020 g. [Elektronnyj resurs] // Ekspertno-analiticheskij centr InfoWatch. 2020. 26 s.
8. Federal'nyj zakon "O kommercheskoj tajne" ot 29.07.2004 No 98-FZ // Rossijskaya gazeta — Federal'nyj vypusk No 0(3543). 05.08.2004.
9. *Despeisse M., Ford S.* The Role of Additive Manufacturing in Improving Resource Efficiency and Sustainability // Centre for Technology Management working paper serie. 2015. No 3. 9 s.
10. *Dilberoglua U.M., Gharehpapagh B., Yaman U., Dolen M.* The role of additive manufacturing in the era of Industry 4.0 // Procedia Manufacturing, 2017. No 11. S. 545–554.
11. *Kasdan Michael J., Smith Kevin M.* Daniels Benjamin Trade Secrets: What You Need to Know // The national law review — Wiggin and Dana LLP, 2019. Vol. IX, № 346.
12. *Moshiria M., Charles A., Elkaseer Ah. e.a.* An Industry 4.0 framework for tooling production using metal additive manufacturing-based first-time-right smart manufacturing system // Procedia CIRP 93 (2020). S. 32–37.
13. *Nesteruk Ph., Kharchenko A., Nesteruk G.* Information safety in electronic business: adaptive model of systems safety of information technologies // Proc. of Int. Conf. "Information technology in business" (St. Petersburg, October 8–10, 2003). St. Petersburg, 2003. P. 124–128.
14. *Zabojnik J.* A theory of trade secrets in firms // International economic review. Vol. 43, Issue 3, 2002. S. 831–855.