ГЛУШКОВ Валентин Алексеевич,
студент Кузбасского гуманитарно-педагогического института федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровский государственный университет»
e-mail: valekpike@gmail.com

БЕЛАРЕВА Ольга Александровна,
научный руководитель,
Кузбасского гуманитарно-педагогического института федерального государственного бюджетного образовательного учреждения высшего образования «Кемеровский государственный университет»
e-mail: belarev@mail.ru

ПРОБЛЕМА ЛЕГАЛИЗАЦИИ ДАННЫХ СОБРАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ DLP, SIEM И DCAP НА ПРЕДПРИЯТИИ И ОРГАНИЗАЦИИ

АННОТАЦИЯ. Данная научная статья посвящена проблеме легализации данных, собранных с использованием систем Data Loss Prevention, Security Information and Event Management и Data-Centric Audit and Protection в деятельности предприятий и организаций. В статье рассматриваются тонкости использования, сбора и последующей обратки полученной информации, представляющей собой коммерческую тайну. Автор проводит анализ существующих правовых норм и предлагает рекомендации по использованию данных систем в соответствии с требованиями законодательства. Также в статье освещаются возможные юридические риски и проблемы, связанные с использованием DLP, SIEM и DCAP, а также предлагаются пути их решения. Исследование проведено на основе анализа законодательства Российской Федерации, а также международных стандартов и рекомендаций в области информационной безопасности. Результаты исследования могут быть полезны предприятиям и организациям, занимающимся внедрением и использованием систем DLP, SIEM и DCAP, а также специалистам в области информационной безопасности и юристам, занимающимся вопросами защиты данных.

КЛЮЧЕВЫЕ СЛОВА: компьютерное преступление, доказательство, информационная безопасность, DLP, SIEM, DCAP, коммерческая тайна.

GLUSHKOV Valentin Alekseevich,
Student Kuzbass Humanitarian Pedagogical Institute of the Federal State Budgetary Educational Institution of Higher Education “Kemerovo State University”

BELAREVA Olga Alexandrovna
Scientific supervisor,
Kuzbass Humanitarian Pedagogical Institute of the Federal State Budgetary Educational Institution of Higher Education “Kemerovo State University”

THE PROBLEM OF LEGALIZATION OF DATA COLLECTED USING DLP, SIEM AND DCAP SYSTEMS IN AN ENTERPRISE AND ORGANIZATION

ANNOTATION. This scientific article is devoted to the problem of legalization of data collected using Data Loss Prevention, Security Information and Event Management and Data-Centric Audit and Protection systems in the activities of enterprises and organizations. The article discusses the subtleties of using, collecting and then returning the received information, which is a trade secret. The author analyzes

the existing legal norms and offers recommendations on the use of these systems in accordance with the requirements of the legislation. The article also highlights possible legal risks and problems associated with the use of DLP, SIEM and DCAP, as well as suggests ways to solve them. The study was conducted on the basis of an analysis of the legislation of the Russian Federation, as well as international standards and recommendations in the field of information security. The results of the study can be useful to enterprises and organizations involved in the implementation and use of DLP, SIEM and DCAP systems, as well as information security specialists and lawyers dealing with data protection issues.

KEY WORDS: computer crime, evidence, information security, DLP, SIEM, DCAP, trade secret.

В последние годы с ростом угроз информационной безопасности предприятий и организаций, все более важным становится использование современных систем защиты данных. Системы Data Loss Prevention (далее – DLP), Security Information and Event Management (далее – SIEM) и Data-Centric Audit and Protection (далее – DCAP) являются ключевыми инструментами в области информационной безопасности, которые помогают предотвращать утечки данных, обнаруживать инциденты и защищать конфиденциальную информацию. Цель научной статьи рассмотреть правовые аспекты использования данных систем в деятельности предприятий и организаций, вопросы, связанные с легализацией данных, собранных при помощи вышеперечисленных систем, с соблюдением законодательства о защите данных, правами субъектов персональных данных. Понимание этих правовых аспектов является важным для эффективного внедрения и использования систем DLP, SIEM и DCAP и обеспечения информационной безопасности предприятий и организаций.

Для более подробного разбора данной проблемы следует дать определения указанным системам защиты информации. DLP — это система, которая предназначена для предотвращения утечки конфиденциальных данных и контроля за их использованием в организациях, вне зависимости от формы их собственности.

SIEM – это система, которая объединяет данные о безопасности и событиях в компьютерной сети для мониторинга, обнаружения и анализа потенциальных угроз и атак на информационную систему. Оснащена сканером сети, который визуализирует данные о каждом хосте – устройстве, программе или порте, которые передают сигналы о событиях безопасности. Для удобства сканер сети дополняет карта подключений: она показывает, какие пользователи активны на каком оборудовании.

DCAP – решение для автоматизированного аудита файловой системы, поиска нарушений прав доступа и отслеживания изменений в критичных данных. Архив, созданный данной системой, помогает в расследованиях инцидентов и гарантирует восстановление потерянной информации.

Для каждой компании, применяющей системы DLP, SIEM И DCAP, недостаточно просто внедрить её у себя. Необходимо в компании разработать ряд нормативных локальных актов компании, запустить их в работу и следить за их исполнением.

Приведу некоторый перечень нормативных локальных актов, которые помогут компании использовать DLPсистему, и применять её на законных основаниях с последующей защитой компанией своих интересов. Наименование и перечень нормативных локальных документов не является исчерпывающим и носит рекомендательный характер:

Положение о коммерческой тайне. Один из обязательных документов в компании. Регулирует положения об отнесении информации к коммерческой тайне с указанием перечня информации и применении к ней режима «конфиденциальности».

Положение должно включать в себя: перечень сотрудников, которые имеют доступ к коммерческой тайне; положения об охране коммерческой тайны и способах её охраны; запрет на её разглашение и запретные способы разглашения (обязательно должен быть включен в запрет мессенджеры и пересылки на личную почту работника); информацию о сроке, в течение которого работнику запрещено разглашать коммерческую тайну; - информацию об установленном в компании сроке запрета на раскрытие информации; - иные положения, которые компания считает необходимым отразить в данном документе.

В случае отсутствия такого документа компания не сможет доказать, что информация, которую разгласил работник, является конфиденциальной.

Положение о персональных данных. Один из обязательных документов, который регулирует в компании порядок обработки и хранения персональных данных, способы их защиты. Может включать иные положения, которые компания считает необходимым отразить в данном документе.

Согласие/обязательство работника об ознакомлении его с положениями о коммерческой тайне и положением о персональных данных и обязательством не допускать разглашения.

Инструкция по работе с периферийными устройствами (флешка, внешний жесткий диск, мобильный телефон, планшет и т.д.).

Должен содержать: перечень устройств, которые работник может подключать к рабочему компьютеру и какими способами; перечень устройств, запрещенных к подключению; правила копирования информации на устройства и т.д.

Инструкция по работе с конфиденциальной информацией. Должна включать в себя правила: хранения на рабочем компьютере информации в запароленной папке; хранения конфиденциальных документов на бумажных и цифровых носителях, в сейфе; уничтожения информации на бумаге через шредер; удаления папок в рабочем компьютере особым способом; иные правила, которые применимы компанией в работе.

Но данная инструкция должна быть рабочей, т.е. компания обязана обеспечить работника всем необходимым для соблюдения требований данной инструкции.

Пункт об охране и недопущения работником разглашения конфиденциальной информации и персональных данных в трудовом договоре. При внесении подобного пункта необходимо указать, что работник имеет доступ к конфиденциальной информации и/или персональным данным в силу исполнения им своих должностных обязанностей.

Уведомление работника о применении в компании технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технических устройств (программных или программно-аппаратных) для предотвращения утечек. Важно обязательно получить от работника подпись на уведомлении.

Документы, содержащие положения и процедуры информационной безопасности. Они должны рассказывать об общей политике информационной безопасности, правилах парольной защиты, разграничении контролей доступа, защите от вредоносного программного обеспечения, допустимом использовании информационных систем и сервисов (в т.ч. сети Интернет и корпоративной почты), мониторинге и контроле, управлении инцидентами, процедурах обучения и повышения осведомленности и другую важную информацию.

Инструкции для работников по использованию информационных систем, сервисов и средств защиты информации.

Положение о привлечении работника к ответственности за нарушение им нормативных локальных документов компании. Это может быть единый документ или пунктами включаться в отдельные разделы других нормативных локальных документов компании.

Положение об обработке и защите информации и использовании средств мониторинга. Документ должен регулировать правила обработки и защиты информации (может быть отдельным документом или включаться в вышеуказанные документы в виде разделов).

Любые применяемые к работнику в компании нормативные локальные акты должны быть: представлены работнику для ознакомления; размещены в доступном для всех работников месте (внутренняя папка на диске, сайт для работников и т.д.).

Компания должна получить от каждого работника по каждому применяемому к работнику акту письменное согласие/обязательство/уведомление с подписью работника. В случае если работник отказывается предоставить подписанное согласие/обязательство/уведомление, то компания вправе отказать работнику в доступе к информации, на которую не представлено согласие. В этом случае работник будет иметь ограниченный доступ к информации компании, который может быть отражен в приказе на данного работника.

Так же можно дать рекомендации по факту обнаружения инцидента.

Шаг 1. Уведомление работников. Компании необходимо ознакомить работников, командированных работников, подрядчиков и т.д. (далее - работник) со своими внутренними локальными документами, регулирующими действия с Информацией и ознакомить их под личную подпись. Получить от работников подписанные ими лично согласия о неразглашении Информации. Рекомендуем указать в согласиях привлечение работника к ответственности (дисциплинарная, административная, материальная и уголовная). Сообщить работникам, что все их действия фиксируются, ведется их учет и получить от указанных лиц личную подпись о том, что они уведомлены о данной процедуре.

Шаг 2. Действия при обнаружении инцидента. При обнаружении инцидента сотрудник составляет докладную записку на имя руководителя. Руководитель издает приказ о создании комиссии для служебного расследования. Работнику, допустившему инцидент, направляется уведомление с требованием предоставить письменные объяснения по произошедшему. Работник предоставляет письменные объяснения с описанием обстоятельств инцидента. При отказе работника от предоставления объяснений составляется соответствующий акт. Комиссия проводит

расследование и составляет акт о результатах с указанием всех выявленных обстоятельств. Работник должен ознакомиться с этим актом; при отказе составляется акт об отказе ознакомления. При установлении вины работника руководство принимает решение о применении дисциплинарных мер (замечание, выговор, увольнение). При отказе работника ознакомиться с приказом составляется акт об отказе. От членов комиссии, свидетелей и работника желательно получить обязательства о неразглашении информации, ставшей известной в ходе расследования.

Шаг 3. Работа комиссии проведению служебного расследования. Комиссия при проведении служебного расследования обязана собрать все доказательства, подтверждающие или опровергающие вину работника. Доказательства должны быть получены в срок, указанный в приказе о назначении комиссии. Показания свидетелей фиксируются письменно в присутствии комиссии и подписываются свидетелями и членами комиссии. Письменные документы, включая объяснительные записки работника и прочую документацию, изымаются в присутствии двух свидетелей и работника на его рабочем месте с составлением акта изъятия, подписанного всеми участниками. Электронные доказательства (скриншоты, переписки, данные из программ безопасности) фиксируются работником отдела безопасности в присутствии членов комиссии, двух свидетелей и работника. Если материалы планируется использовать в суде, фиксация проводится в присутствии нотариуса, который удостоверяет и заверяет отчет. При необходимости комиссия направляет запросы разработчику ПО для уточнения технических характеристик и извлечения сведений, относящихся к инциденту.

Шаг 4. Технические сведения. Комиссия может извлечь из программного обеспечения следующие технические сведения: скриншоты рабочего стола на момент инцидента; аудит операций на файловой системе; аудит нажатых клавиш; аудит активности в программном обеспечении и на сайтах (с учетом времени и длительности); теневые копии файлов, переданные пользователем по электронным каналам; информацию об учетных записях пользователя в ИТ системах. Комиссия получит технические сведения в виде печатных материалов либо выгрузки информации в популярных форматах doc, xls, pdf, jpeg, mp3 или в ином доступном формате. Срок хранения информации по действиям работников в рабочем компьютере устанавливается компанией.

Шаг 5. Привлечение к ответственности виновного. Работник, вина которого доказана в совершении инцидента, может быть привлечен руководством компании к следующим видам ответственности: дисциплинарная, материальная (при передаче служебного дела правоохранительным органам – административная и уголовная). 1) Дисциплинарная ответственность: Компания вправе расторгнуть трудовой договор по своей инициативе, если работник разгласит Информацию. Условие: работник узнал Информацию в связи с исполнением трудовых обязанностей (подп. «в» п. 6 ст. 81 ТК РФ [2]). Помимо увольнения, компания вправе применить дисциплинарное взыскание в виде замечания или выговора (ст. 192 ТК РФ). Руководство компании составляет приказ о расторжении трудового договора и знакомит с ним виновного работника. В случае отказа виновного работника от подписания приказа составляется акт об отказе в ознакомлении с приказом о прекращении трудового договора с виновным работником. 2) Материальная ответственность: Работник, который разгласил Информацию, несет материальную ответственность в полном размере причиненного ущерба. Закон не запрещает за один проступок одновременно применять материальное и дисциплинарное взыскание. 3) Административная ответственность: Лицо, которое получило доступ к Информации, когда исполняло служебные или профессиональные обязанности, может быть привлечен к ответственности, если разгласит такую Информацию. Штраф для должностных лиц установлен КоАП РФ. 4) Уголовная ответственность: Суд назначит исправительные или принудительные работы, лишающие права занимать виновному работнику соответствующие должности. В виде дополнительного наказания может назначаться штраф. В исключительных случаях виновного работник могут лишить свободы.

В качестве примеров различных видов ответственности можно привести следующие примеры. Сотрудник был уволен по подпункту «в» пункта 6 части первой статьи 81 Трудового кодекса РФ. Согласно разъяснениям, содержащимся в п.43 Постановления Пленума Верховного Суда Российской Федерации № 2 от 24.11.2015 г. «О применении судами Российской Федерации Трудового кодекса Российской Федерации [3]», в случае оспаривания работником увольнения по подпункту «в» пункта 6 части первой статьи 81 Кодекса работодатель обязан представить доказательства, свидетельствующие о том, что сведения, которые работник разгласил, в соответствии с действующим законодательством относятся к государственной, служебной, коммерческой или иной охраняемой законом

тайне, либо к персональным данным другого работника, эти сведения стали известны работнику в связи с исполнением им трудовых обязанностей и он обязывался не разглашать такие сведения.

Работник уволен за отправку, с корпоративной электронной почты на личную почту работника электронного письма, содержащего условия договоров с контрагентами, величину задолженности и лимиты по договорам [5]. Работодатель доказал и обосновал принятое решение об увольнении работника, аргументируя свои действия подписанными работником документами об ознакомлении с конфиденциальной информацией и выраженным в письменном виде согласием на неразглашение конфиденциальной информации.

Сотрудница полиции уволена за распространение фото и данных несовершеннолетней потерпевшей через «Вконтакте», WhatsApp, Instagram [6]. Для конкретного дела не имеет значения, кто начал распространять данные. Сотрудница полиции не имела права пересылать своим знакомым ориентировку по преступлению, которое совершили в отношении несовершеннолетней.

Работника уволили за то, что им на свой электронный почтовый ящик действительно отправлены письма, содержащие рабочие вложения программного обеспечения, полученного им для работы над программным обеспечением заказчика, но сделано это с разрешения его начальника для того, чтобы ускорить выполнение производственного задания. Отправленную информацию работник не считает коммерческой тайной, т.к. информация находится в свободном доступе в сети интернет [7]. Суд пришел к правильному выводу об отсутствии оснований для удовлетворения иска, поскольку работник, имея доступ к информации, составляющей коммерческую тайну и представляющую ценность для работодателя, отправил себе на личную почту интерфейс программирования приложений RSSQL.

Руководитель группы в кол-центре незаконно снимала копии паспортов стажеров и соискателей. Она нарушила один из пунктов положения о коммерческой тайне, который относит к конфиденциальной информации персональные сведения о подготовке и обучении кадров. Работодатель применил к работнице дисциплинарное взыскание в виде замечания [8]. Суд признал законным решение работодателя применить дисциплинарное взыскание в виде замечания за нарушение положения о коммерческой тайне.

Работника уволили за разглашение сведений, составляющих коммерческую тайну, а потом еще судили по ст. 183 УК РФ [1] (Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, ч1 и ч2) [4]. Суд признал работника виновным по ч.1 и ч.2 ст. 183 УК РФ и назначил наказание в виде 1 года 9 месяцев исправительных работ с удержанием из заработка ежемесячно 15% в доход государства.

Работник обратился в суд с иском в отношении работодателя о признании незаконным приказа о расторжении трудового договора, об обязательстве не чинить препятствия к осуществлению трудовой деятельности и допустить к работе, о взыскании денежной компенсации за время вынужденного прогула и компенсации морального вреда [9]. Исковые требования работника судом не удовлетворены. Выдержка из Решения суда: «Согласно п.п. 4.6, 4.7, 4.15 указанной должностной инструкции истец обязан был участвовать в разработке основополагающих документов с целью закрепления в них требований обеспечения сохранности имущества и защиты коммерческой тайны…»

Работник обратился с иском в суд к работодателю о признании незаконным п. 4 и п. 5 Заключения служебной проверки, признании незаконным и отмене дисциплинарного взыскания в виде выговора, наложенного приказом от < Дата > №, взыскании невыплаченной премии, о признании незаконным и отмене дисциплинарного взыскания в виде замечания, наложенного приказом от < Дата > №, о признании незаконными выводов и предложений заключения служебной проверки, признании незаконным и отмене дисциплинарного взыскания в виде увольнения, наложенного приказом от < Дата > №-к/5500, восстановлении на работе, взыскании среднего заработка за время вынужденного прогула, компенсации морального вреда [10]. Суд отказал в полном объеме работнику в исковых требованиях, т.к. работодатель доказал факт копирования конфиденциальной информации на съемный диск. Выдержка из Решения суда: Судом было установлено, что в соответствии с Регламентом взаимодействия структурных подразделений Компании при использовании DLP-системы осуществляется контроль использования внешних (съемных) носителей информации, включая протоколирование и аудит использования устройств на локальном компьютере отдельными пользователями и группами пользователей посредством ведения журнала аудита, используемого для хранения записей протокола доступа пользователей к устройствам, подпавшим под заявленные правила аудита, в который записываются все изменения в настройках DL (хранение информации 7 суток), а также журнала теневого копирования, используемого для хранения файлов, которые

были скопированы, изменены, отправлены на печать на рабочих местах пользователей, которые были внесены в группу теневого копирования (срок хранения информации не менее 60 суток).

Так же можно привести в пример ситуацию, где непосредственно в материалах дела будет ссылка на системы предотвращения утечек информации. Группа лиц по предварительному сговору с целью дальнейшей продажи сведений заинтересованным лицам осуществила сбор сведений, составляющих коммерческую тайну незаконным путем. Лица, входящие в группу лиц по предварительному сговору, признаны виновными в совершении преступления, предусмотренного ч.3 ст.183 УК РФ, и на основании санкции данной статьи суд назначил наказание в виде лишения свободы. Выдержка из Приговора суда: «Свидетель ФИО пояснил суду, что работает в ПАО «ХХХ» в должности ведущего специалиста отдела защиты тайны связи и безопасности информации Единого центра комплексной безопасности, в обязанности входит просмотр инцидентов, регистрируемых корпоративной системой обнаружения утечек конфиденциальной информации (система DLP), предварительный анализ инцидентов и отправке службе безопасности в регионы по всей России, доступ в данную систему имеется на рабочем компьютере, она фиксирует уход информации с рабочей почты сотрудников, мониторинг информации и фиксирует факты неправомерного запроса этой информации, отсеивает инциденты с признаками неправомерной отправки, после чего он просматривает на своем компьютере наличие конфиденциальной информации, которая определена специальной политикой безопасности компании и ФЗ «О коммерческой тайне», с автоматически настроенных политик.»

Во всех вышеприведенных примерах можно увидеть тенденцию, что суды почти всегда встают на сторону работодателя так как в случае подготовленной базы локально правовых актов действия злоумышленника довольно просто доказать, тем самым облегчить проведения расследования, и так же поспособствовать привлечению к ответственности.

Однако при столь большом многообразии юридического обоснования использования систем DLP, SIEM и DCAP на данный момент существует проблема по легализации данных, полученных при помощи данных систем. Выше были перечислены правила, рекомендации, нормативы и другая документация при использовании которой администрация организации избежит всех проблем правового характера. Однако мало людей при ознакомлении полностью читают локально нормативные акты, что приводит в будущем к неприятным последствиям для сотрудника в случае нарушения одного из пунктов положений. Это может быть как административная ответственность, так и уголовная. Например, сотрудник А, занимающий должность специалиста отдела снабжения организации «Amber» при приеме на работу в момент ознакомления с локально нормативными актами, подписал все, не прочитав и не ознакомившись с содержанием данных документов. Одним из которых было «Обязательство о неразглашении конфиденциальной информации и соблюдении правил ее обработки». В один из дней представитель смежной компании решила прийти с дружеским визитом и увидев расспросить как у них дела в компании. Сотрудник рассказал все что знал и это зафиксировали камеры видеонаблюдения и в последствии сведения были переданы в службу безопасности. Было назначено служебное расследование служебного инцидента по факту нарушения локально нормативных актов «Amber». В ходе расследования бы выяснено, что кроме локально нормативных актов была также нарушена Статья 183 УК РФ Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. В последствии собранные материалы расследования были переданы правоохранительным органам. Из данного примера можно сделать вывод, что небрежность и легкомыслие по отношению к документам который подписывает будущий сотрудник может привести к неблагоприятным последствиям.

Однако в случае недостаточной нормативно базы локально нормативных актов, организация несет экономические и репутационные риски, и не сможет рассчитывать на компенсацию своих рисков в случае инцидента. Так, например, сотрудник Б отдела бухгалтерии компании «Tupe», при приеме на работу уделил значительное время для изучения локально нормативных актов, полностью с ними ознакомился и подписал. В последствии через 4 месяца пригласил на обед в столовую компании своего друга и в течении отведенного времени для отдыха поделился информацией, причисленной к коммерческой тайне. Этот разговор услышал работник департамента безопасности, и вскоре было назначено служебное расследование на предмет нарушения отдельных пунктов локально нормативных актов. Однако в компании отсутствовали документы, регламентирующие применение систем DLP, SIEM и DCAP для сбора информации и выявления инцидентов, направленных на информационную безопасность организации. Но в ходе служебного расследова-

ния выяснилось, что кроме пунктов ЛНА было нарушено в том числе и УК РФ, и начальник отдела департамента принял решение о передаче собранных сведений в правоохранительные органы. При проверке материалов было выяснено, информация была собрана при помощи данных систем и в том числе при помощи специальных технических средств, предназначенных для негласного получения информации. В последствии на начальника департамента безопасности, и всех лиц, занимавшихся им, было возбуждено уголовное дело по статьям Статья 138.1 УК РФ Незаконный оборот специальных технических средств, предназначенных для негласного получения информации, и Статья 137. УК РФ Нарушение неприкосновенности частной жизни, и они были привлечены к ответственности. Позже при проведении расследования правоохранительными органами, из-за недостаточных оснований для привлечения к уголовной ответственности было прекращено уголовное расследование, и сотрудник Б избежал наказания за содеянное. Из данного примера можно сделать вывод, что для легального использования в компании данных систем защиты от утечек информации, следует разрабатывать полную нормативную базу локально нормативных актов, так как в случае какого-либо инцидента компания не только понесет экономические и репутационные потери, но и может быть принужденно к выплате компенсации за противоправное использование систем DLP, SIEM и DCAP.

В заключение, проблема легализации данных, собранных с использованием систем DLP, SIEM и DCAP на предприятии и организации, имеет важное значение в современном мире информационных технологий. Несмотря на неоднозначность мнений и разнообразие правовых регламентов в разных компаниях, необходимость регулирования процесса сбора, хранения и управления данными становится все более актуальной. При использовании систем DLP, SIEM и DCAP предприятия и организации получают значительные преимущества в области информационной безопасности и контроля конфиденциальности данных. Поэтому компании следует сосредоточиться на проведении детального анализа юридической и нормативной среды, в которой они действуют, и разработать специализированные стратегии легализации данных для каждого конкретного рынка. Кроме того, стоит уделить должное внимание документированию процессов сбора, обработки и управления данными. Следует также разработать четкие правила и процедуры для сотрудников, чтобы гарантировать соблюдение всех требований в области безопасности данных и обеспечить их доступность и доступность только авторизованным лицам.

Список литературы:

[1] «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 14.02.2024)// «Российская газета», N 113, 18.06.1996, N 114, 19.06.1996, N 115, 20.06.1996, N 118, 25.06.1996.

[2] «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 14.02.2024)// «Собрание законодательства РФ», 07.01.2002, N 1 (ч. 1), ст. 3.

[3] Постановление Пленума Верховного Суда РФ от 17.03.2004 N 2 (ред. от 24.11.2015) «О применении судами Российской Федерации Трудового кодекса Российской Федерации»// «Бюллетень Верховного Суда РФ», N 6, 2004.

[4] Апелляционное постановление № 10-7264/2013 от 15 августа 2013 г. по делу № 1-160/13 Московский городской суд / [Электронный ресурс] // Официальный портал судов общей юрисдикции города Москва : [сайт]. — URL: https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/2779875a-9377-488b-b091-961341573065 (дата обращения: 26.03.2024).

[5] Дело № 33-17995/2017 Мещанский районный суд г. Москва / [Электронный ресурс] // Официальный портал судов общей юрисдикции города Москва : [сайт]. — URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/61904374-5927-4d47-8fd1-e32d65e59615 (дата обращения: 26.03.2024).

[6] Дело № 33-1723/2018 Тимирязевский районный суд г. Москва / [Электронный ресурс] // Официальный портал судов общей юрисдикции города Москва : [сайт]. — URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/4fed13ac-5b13-4f1c-9af9-a8706e53114d (дата обращения: 26.03.2024).

[7] Дело № 33-4610/2017 Московский городской суд / [Электронный ресурс] // Официальный портал судов общей юрисдикции города Москва : [сайт]. — URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/243bd76f-5af9-4bda-a2c6-43e6755b350b (дата обращения: 26.03.2024).

[8] Дело № 33-4524/2017 Санкт-Петербургский городской суд / [Электронный ресурс] // Судебные решения РФ : [сайт]. — URL: https://судебныерешения.рф/69115486 (дата обращения: 26.03.2024).

[9] Решение № 2-1369/2019 2-1369/2019~М1594/2019 М-1594/2019 от 4 июля 2019 г. по делу № 2-1369/2019 / [Электронный ресурс] // Официальный портал судов общей юрисдикции города Москва : [сайт]. — URL: https://mos-gorsud.ru/rs/koptevskij/services/cases/civil/details/621821a3-d214-4425-a692-104f36cd9a05 (дата обращения: 26.03.2024).

[10] Решение № 2-1610/2018 2-1610/2018~М502/2018 М-502/2018 от 9 июля 2018 г. по делу № 2-1610/2018/2018 от 9 июля 2018 г. по делу № 2-1610/2018 / [Электронный ресурс] // СудАкт : [сайт]. — URL: https://sudact.ru/regular/doc/myQ1LLeFdbrs/ (дата обращения: 26.03.2024).

Spisok literatury:

[1] "Criminal Code of the Russian Federation" dated 13.06.1996 N 63-FZ (as amended by 14.02.2024) //Rossiyskaya Gazeta, N 113, 18.06.1996, N 114, 19.06.1996, N 115, 20.06.1996, N 118, 25.06.1996.

[2] "Labor Code of the Russian Federation" dated 30.12.2001 N 197-FZ (as amended on 14.02.2024) //" Collection of Legislation of the Russian Federation, "07.01.2002, No. 1 (part 1), Art. 3.

[3] Resolution of the Plenum of the Supreme Court of the Russian Federation of 17.03.2004 No. 2 (ed. 24.11.2015) "On the Application of the Labor Code of the Russian Federation by the Courts of the Russian Federation "//Bulletin of the Supreme Court of the Russian Federation, No. 6, 2004.

[4] Appeal Decision No. 10-7264/2013 of August 15, 2013 in case No. 1-160/13 Moscow City Court/[Electronic Resource]//Official Portal of Courts of General Jurisdiction of the City of Moscow: [website]. - URL: https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/2779875a-9377-488b-b091-961341573065 (access date: 26.03.2024).

[5] Case No. 33-17995/2017 Meshchansky District Court of Moscow/[Electronic Resource]//Official portal of courts of general jurisdiction of the city of Moscow: [website]. - URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/61904374-5927-4d47-8fd1-e32d65e59615 (access date: 26.03.2024).

[6] Case No. 33-1723/2018 Timiryazevsky District Court of Moscow/[Electronic Resource]//Official portal of courts of general jurisdiction of the city of Moscow: [website]. - URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/4fed13ac-5b13-4f1c-9af9-a8706e53114d (access date: 26.03.2024).

[7] Case No. 33-4610/2017 Moscow City Court/[Electronic Resource]//Official portal of courts of general jurisdiction of the city of Moscow: [website]. - URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/243bd76f-5af9-4bda-a2c6-43e6755b350b (access date: 26.03.2024).

[8] Case No. 33-4524/2017 St. Petersburg City Court/[Electronic Resource]//Court decisions of the Russian Federation: [website]. - URL: https://судебныерешения.рф/69115486 (access date: 26.03.2024).

[9] Decision No. 2-1369/2019 2-1369/2019 ~ M1594/2019 M-1594/2019 dated July 4, 2019 in case No. 2-1369/2019/[Electronic resource]//Official portal of courts of general jurisdiction of the city of Moscow: [website]. - URL: https://mos-gorsud.ru/rs/koptevskij/services/cases/civil/details/621821a3-d214-4425-a692-104f36cd9a05 (access date: 26.03.2024).

[10] Decision No. 2-1610/2018 2-1610/2018 ~ M502/2018 M-502/2018 dated July 9, 2018 in case No. 2-1610/2018/2018 dated July 9, 2018 in case No. 2-1610/2018/[Electronic resource]//CourtAct: [website]. - URL: https://sudact.ru/regular/doc/myQ1LLeFdbrs/ (access date: 26.03.2024).