Проблемы дефиниций и постановки целей защиты от утечек информации ограниченного доступа

Г.В. Гарбузов

***Аннотация*— В настоящей статье рассматриваются проблемные методологические вопросы, возникающие в процессе научной организации защиты информации ограниченного доступа от утечки и разглашения. В частности, отмечается недостаточность проработки терминологии в отечественном законодательстве и её противоречивость в отраслевом, которое предлагает различные, подчас противоречащие друг другу определения. Постановка задачи: определить баланс подходов к защите информации ограниченного доступа в организации, определить критерии утечки информации ограниченного доступа как специфического вида угроз информационной безопасности. Результаты: авторы провели исследования с целью выбора целевого подхода к определению утечки информации и его взаимосвязи с разглашением информации ограниченного доступа, кроме того, в статье определены подходы к определению объектов защиты – информации ограниченного доступа – ценностный и регуляторный, а также определены ключевые аспекты, которые должны быть учтены в дальнейшем при разработке комплексной системы защиты информации ограниченного доступа от утечек. Практическая значимость: предложенные подходы могут использоваться специалистами коммерческих и некоммерческих организаций при построении моделей угроз информации ограниченного доступа и построении систем защиты информации ограниченного доступа. Обсуждение: представлено одно из направлений определения подходов к защите от утечек информации, важно продолжить синхронизацию понятийного аппарата в отечественном законодательстве и отраслевом направлении.**

***Ключевые слова*— информация ограниченного доступа, утечка информации, защита от утечки информации, разглашение информации, нематериальный актив, коммерческая тайна, Data Leak Protection, защита информации.**

I. Введение

Информация занимает важное место в структуре экономики любого современного предприятия, выступая в роли как товара, так и ресурса. Информация как средство производства способна снизить себестоимость продукции и избежать излишних издержек, при этом она не уничтожается в процессе личного или производственного потребления, являясь неисчерпаемым и неограниченным ресурсом. Расширение использования информации как производственного ресурса в постиндустриальном (информационном) обществе является катализатором трансформации производственных отношений и формирования цифровой экономики, приход которой имеет ряд важных последствий, в частности, стирание границ территорий и растущую роль информации и информационных технологий в экономических отношениях. В цифровой экономике, в противовес классической (промышленной), производство и потребление смещается в сторону услуг, а информация является одновременно и товаром, и средством производства. Информация как товар (информационный продукт, например, программное обеспечение, базы данных, или услуга, например, образовательные услуги, консультирование) способна удовлетворить запрос потребителя, при этом к источнику информации могут обратиться неограниченное количество потребителей и неограниченное количество раз.

Законодательство Российской Федерации допускает свободное использование информации юридическими и физическими лицами, а также её свободную передачу между ними, за исключением случаев, когда такое использование ограничено законом [1]. В этом случае информацию называют информацией ограниченного доступа (также, «ограниченного распространения», «конфиденциального характера», в некоторых случаях «защищаемой информацией») и она имеет особую ценность уже не только как производственный ресурс и актив предприятия, но и как объект защиты от релевантных угроз.

Для информации, как для специфического актива, актуальны специфические же угрозы, одной из самых существенных из которых является т.н. утечка информации, в результате которой информация может обесцениться и, в случае если информация являлась основным активом предприятия (например, наукоёмких производств, широко использующих объекты интеллектуальной собственности), даже поставить предприятие на грань банкротства [1]. Анализ утечек

Статья получена 31 марта 2024.

Гарбузов Георгий Валерьевич – аспирант Финансового университета при Правительстве Российской федерации, ORCID: http://orcid.org/0009-0008-7717-1488 (e-mail: g.garbuzov@mail.ru)

[1] Например, банкротство финской сети психотерапевтических центров Vastaamo в 2021 или банкротство Cambridge Analytica вследствие утечки данных из Facebook в 2018. Утечка привела к банкротству // Infowatch. 15 сентября 2023. https://www.infowatch.ru/analytics/utechki-informatsii/utechka-privela-k-bankrotstvu

Cambridge Analytica обанкротится из-за скандала с данными Facebook // Ведомости. 02 мая 2018.

информации в мире за прошедшие два года, согласно свежему отчету отечественных аналитических центров[2], показывает, что количество утечек в 2023 году на 65% превысило показатели 2022 года, а объем утечек корпоративных данных (т.е. информации, являющейся активом предприятия – интеллектуальной собственности, секретов производства, коммерческой тайны и пр.) в общем объеме утечек вырос почти втрое относительно того же периода.

Защита от утечек информации является критически важным элементом безопасности для всех участников цифровой экономики и должна осуществляться комплексно, включая в себя меры правового, организационного и технического характера. Научный подход к построению комплексной, масштабируемой и эффективной в долгосрочном горизонте системы защиты конфиденциальности информации должен включать проработку всех основных элементов:

- Правового: границы ответственности субъекта, реализующего или способствующего реализации угроз безопасности в отношении объекта защиты (информации).
- Социального: согласно концепции Zero Trust, сегодня каждый субъект (работник организации, партнер, официальное лицо) должен рассматриваться как потенциальная угроза и нарушитель конфиденциальности.
- Технического: меры защиты информации от утечки должны быть реализованы на всех этапах её жизненного цикла, при этом особое внимание следует уделить надежной идентификации объекта защиты (информации). Используются как средства общего назначения, так и специализированные системы, такие как DLP [2]. Всё большее значение в борьбе с утечками приобретают высокие технологии, такие как искусственный интеллект, который на сегодняшний день является наиболее перспективным решением и всё чаще используется в построении режимов коммерческой и иной тайн в организации[3] [3, 4].
- Организационного: прежде всего, работа с персоналом, включая входной скрининг, обучение, выявление девиантного поведения, а также развитие процессов управления информационной безопасностью, включая разработку и применение передовых методов оценки рисков информационной безопасности [5].
- Этического: использование технологий в процессах, имеющих юридические последствия и влияющих на процесс принятия решений в отношении прав и свобод человека, должно оцениваться с этической точки зрения. В частности, внедрение новых цифровых технологий, в том числе технологий искусственного интеллекта, требует установления особого правового режима [6].

В настоящей статье рассматриваются некоторые проблемные вопросы методологического характера, а именно определение объекта защиты и определение основных понятий, составляющих методологическую основу всей работы.

II. Определение объекта защиты

Основным способом вовлечения информации в производственный процесс в качестве производственного ресурса или товара является перевод её в разряд нематериальных активов, которые согласно работе [7] определяются как:

1. не имеющие материально-вещественной формы;
2. предназначенные для использования организацией в ходе обычной деятельности при производстве и (или) сбыте ею продукции (товаров), при выполнении работ или оказании услуг, для предоставления за плату во временное пользование, для управленческих нужд либо для использования в деятельности некоммерческой организации, направленной на достижение целей, ради которых она создана;
3. предназначены для использования организацией в течение периода более 12 месяцев или обычного операционного цикла, превышающего 12 месяцев;
4. способны приносить организации экономические выгоды (доход) в будущем (обеспечить достижение некоммерческой организацией целей, ради которых она создана), на получение которых организация имеет право (в частности, в отношении таких активов у организации при их приобретении (создании) возникли исключительные права, права в соответствии с лицензионными договорами либо иными документами, подтверждающими существование права на такие активы) и доступ иных лиц к которым организация способна ограничить;
5. могут быть выделены (идентифицированы) из других активов или отделены от них.

Необходимо обратить внимание на то, что некоторые нормативные акты в конкретных целях, например, для целей проведения оценки нематериальных активов [8], предлагают расширенную формулировку, определяя нематериальный актив (объект оценки) как «исключительные права на результаты интеллектуальной деятельности и (или) приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальная собственность), указанные в статье 1225 Гражданского кодекса Российской Федерации, или права использования таких результатов интеллектуальной деятельности и (или) средств индивидуализации, являющиеся объектами гражданских прав, в отношении которых законодательством Российской Федерации установлена возможность их участия в гражданском обороте, а также аналогичные права на совокупность таких объектов», а также «исключительное право на сложный объект (в соответствии со статьей 1240 Гражданского кодекса Российской Федерации[3]), включающий несколько охраняемых результатов интеллектуальной деятельности или право

https://www.vedomosti.ru/technology/news/2018/05/02/768374-cambridge-analytica

[2] Исследование утечек информации в мире за последние два года // Infowatch. 11 апреля 2024. https://www.infowatch.ru/analytics/analitika/issledovaniye-utechek-informatsii-v-mire-za-posledniye-dva-goda

[3] Подробнее данный аспект будет рассмотрен в следующих публикациях

использования таких объектов. Права (исключительное право и (или) право использования) на отдельные охраняемые результаты интеллектуальной деятельности, входящие в состав сложного объекта, могут выступать в качестве самостоятельных объектов оценки».

Оба этих определения существенны для обозначения объекта и понимания методов его защиты.

На реальное обесценивание нематериального актива (прежде всего секрета производства, информации, составляющей коммерческую тайну) влияет иной набор факторов, нежели на активы материального мира. Информация может испытывать как внутреннее, естественное воздействие (устаревание, утрата актуальности, «моральный износ»), так и внешнее, к которому следует отнести классические угрозы безопасности информации (угрозы конфиденциальности, достоверности, целостности и доступности). При этом с точки зрения невосполнимой утраты ценности нематериального актива одной из наиболее актуальных для конкурентной экономической среды угрозой следует считать угрозу конфиденциальности, поскольку в случае разглашения информации, которое в редакции Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» определяется как «действие или бездействие, в результате которых *информация* становится известной третьим лицам без согласия законного обладателя или вопреки условиям договора», разрушается её ценность, необходимым условием которой, как раз является неизвестность третьим лицам. Последствия реализации угрозы влияют не только на репутацию и финансовое состояние обладателя информации, но и на её потребителя.

Помимо аксиологического (ценностного) аспекта информации, следует также учитывать и её правовой статус: в отношении определенных видов информации, таких как персональные данные, профессиональные тайны, законодательством Российской Федерации прямо введены императивные нормы защиты их конфиденциальности, а также определена ответственность различных субъектов информационного взаимодействия. Например, ст.13.11 КоАП РФ устанавливает ответственность за «действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации», а ст.183 УК РФ – за «собирание сведений, составляющих коммерческую, налоговую или банковскую тайну» и «незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе. Новый законопроект № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» от 04.12.2023 вводит уголовную ответственность за «незаконные использование и(или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения», а законопроект № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 04.12.2023 предусматривает применение оборотных штрафов, составляющих до 3% выручки организации, за «действие (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей персональные данные».

Таким образом, при планировании мер по снижению рисков причинения ущерба вследствие реализации угроз конфиденциальности, следует рассматривать объект защиты (информацию) как минимум с двух аспектов:

1. Как **нематериальный актив**, имеющий коммерческую ценность в силу неизвестности третьим лицам и теряющий её в случае разглашения.
2. Как сведения, которые должны быть защищены apriori, **в соответствии с требованиями закона**, и разглашение которых влечет репутационный ущерб и наложение штрафных санкций, вплоть до приостановки деятельности организации. В этом случае система защиты должна выстраиваться с учетом требований закона.

III. Утечки информации как специфический вид угроз

Реализацию угрозы конфиденциальности информации мы будем называть утечкой информации. Примером последних лет является утечка данных бронирования около 500 миллионов гостей сети отелей Marriott Starwood, обнаруженная в ноябре 2018 года [9], которая привела к выплате штрафа в 23,8 млн. долл. США, кроме того против компании было подано несколько коллективных гражданских исков и она согласилась оплатить замену паспортов клиентов, ставших жертвами утечки. В результате её капитализация (по данным биржевой аналитики [10]) в результате утечки всего за месяц снизилась на 17% (с 41,6 до 34,5 млрд. долл. США). В дополнение к прямому ущербу, в 2019 году снизились показатели удовлетворенности клиентов Marriott Starwood: по этому показателю бренд сравнялся с Hilton, что свидетельствует о нанесении долгосрочного ущерба лояльности гостей.

Причиной описанной утечки, как показало проведенное расследование, явилось стечение факторов как технического, так и организационного характера: устаревшая система бронирования, увольнение ИТ персонала и нехватка контроля за попытками атак, выявленных еще в 2015 году. Анализ ситуации со стороны экспертного сообщества показал, что утечка из Marriott была вопросом времени и, если бы руководство должным образом реагировало на определенные маркеры, ущерба удалось бы избежать.

Описанный случай далеко не единственный, хотя и один из самых масштабных. Согласно данным западных аналитических агентств [11], [12], [13] средняя стоимость утечки в США в 2023 году достигла рекордного уровня 4,45 миллиона долларов США (на 2,3% больше, чем в 2022 году) и в долгосрочной перспективе она увеличилась на 15,3% по сравнению с 2020 годом (3,86 млн долларов США), а 74% всех

нарушений связаны с человеческим фактором – ошибками и халатностью персонала, злоупотреблением привилегиями или социальной инженерией. В России [14] больше всего утечкам были подвержен промышленный сектор и в 70% случае утечки имели умышленный характер.

Однако, необходимо отдельно остановиться на смысле и определении самого понятия – «утечка информации». В законодательстве РФ понятие «утечка информации» на сегодняшний день отсутствует, определено лишь понятие «разглашение информации» (их взаимосвязь рассмотрим чуть позже), терминология утверждена лишь на уровне государственных и отраслевых стандартов. Для начала определим, что утечка всегда связана с движением информации и рассмотрим возможные варианты отношений субъектов информационного взаимодействия, в ходе которого информация (объект защиты) передается из периметра организации за её пределы (Рис. 1).

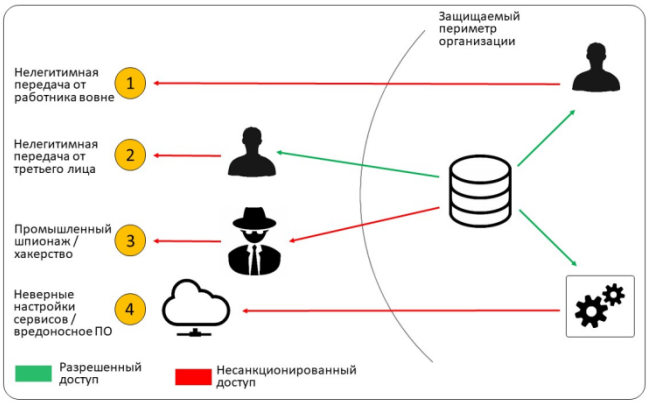

Рис. 1. Схема информационных взаимодействий

Здесь работник организации (в цепочке 1) или третье лицо (в цепочке 2) получают законный (авторизованный) доступ к информации, например, на основании трудового или гражданского договора, после чего в нарушение политик безопасности или договора передают её неустановленному получателю. Возможна также ситуация, при которой внешний злоумышленник, преодолев защитные меры, получает несанкционированный доступ к информации (цепочка 3). И, наконец, нельзя забывать о возможности несанкционированной передачи информации вследствие работы каких-либо неверно сконфигурированных служб или вредоносного ПО (элемент 4).

ГОСТ [15] вводит понятие «Защита информации от утечки», которое определяется как «защита информации от неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами», к числу которых относят «государство, юридическое лицо, группу физических лиц, отдельное физическое лицо». Контексту такой формулировки соответствует цепочка 3 схемы (Рис. 1) и на наш взгляд, поскольку в данной формулировке утечка информации всегда является следствием ее разглашения (т.е., как определили выше, действием, приведшим к ознакомлению третьими лицами) и (!) несанкционированного доступа, круг источников потенциальных угроз оказывается сужен. Например, утечка, допущенная по вине работника, имевшего доступ к информации в соответствии с трудовыми обязанностями или договором, и передавшего её за пределы организации, не имея умысла на разглашение, не подпадает под смысл данного выше определения утечки информации. То же касается и «технологических» причин, например, утечкой в результате неверной конфигурации оборудования или работой вредоносных программ.

В РС БР ИББС-2.9-2016 [16] утечка информации определена как «несанкционированное предоставление или распространение информации конфиденциального характера, не контролируемое организацией БС РФ», то есть смысловая часть объективна и уже не ставит суть понятия в зависимость от чьих-либо действий и мотивов. Однако, поскольку документ имеет узконаправленное, специальное назначение, в документе введено ограничение: он охватывает только случаи утечки информации, допущенные в результате действий инсайдеров (работников банковских организаций) или третьих лиц, которым доступ к этой информации (или в помещения обработки информации) был предоставлен легально, таким образом, реализуя цепочку 1 схемы (Рис. 1). Данное определение, на наш взгляд, обладает еще меньшей универсальностью, ограничивая круг возможных источников угроз не только на отраслевом уровне (только организации БС РФ), но и исключая из рассмотрения, внешних нарушителей, т.е. лиц, получивших к информации несанкционированный доступ (промышленный шпионаж, иностранные разведки и прочие третьи лица), а также упомянутые выше «технологические» причины.

Поскольку из смысла определений утечки (неконтролируемое распространение информации) ясно, что в основе лежит некий процесс передачи информации – распространение, всегда подразумевающий наличие канала распространения, можно констатировать, что утечка создает условия и предпосылки для **разглашения** (т.е. **ознакомления** кем-либо), предшествует ему, при этом неважно, как именно информация была разглашена – даже если она была просто «выболтана», разглашению в данном предшествовала утечка информации в виде допуска нелояльного (в этом проявляется критерий недостатка контроля) субъекта к конкретным секретам.

Законопроект № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 04.12.2023 в качестве нарушения рассматривает «действие (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей персональные данные». Фактически имея в виду утечку информации, данное определение опускает фактор контроля за распространением информации, упоминаемое в двух предыдущих, что позволяет сделать вывод о потенциальной возможности контролируемого

(т.е., исходя из смысла понятия «контроль» - наблюдаемого), несанкционированного распространения. Это, на наш взгляд, противоречит смыслу, изначально вкладываемому в понятие «утечка информации», предполагающему утрату контроля за информацией и отсутствие каких-либо данных о её перемещении, копировании, сохранении и т.д.

Поскольку защита от утечек должна строиться комплексно, с учетом всех возможностей несанкционированной передачи информации, т.е. предусматривая все элементы схемы (Рис. 1), целесообразно окончательно определить утечку информации как **несанкционированное и не контролируемое обладателем распространение информации ограниченного доступа**, которое, в свою очередь, может быть определено как **действия, направленные на получение этой информации ограниченным или неограниченным кругом лиц** (соответственно). Данное определение свободно от причин получения доступа к информации и типа субъекта, допустившего утечку, при этом утечка информации логически предваряет и создает предпосылки для разглашения информации, которое, в свою очередь, означает, что информация вследствие утечки стала известна третьим лицам вопреки договору или без согласия законного обладателя. Обращаем внимание на важное обстоятельство: объективная сторона правонарушения, именуемого «разглашение информации» обязательно включает в себя ознакомление с этой информацией не допущенным к ней лицом. Если ознакомления не было, нельзя говорить и о разглашении, простого «доступа» или «создания условий для ознакомления» здесь недостаточно. Отметим также, что в зависимости от мотивации субъекта утечки могут быть умышленными (корыстные мотивы, промышленный шпионаж, социальный протест и др.) и неумышленными (неосведомленность о правилах безопасности, ошибки интерпретации или саботаж требований по защите информации). Не будем также забывать об утечках информации, возникших по упомянутым выше «технологическим» причинам (т.е. без непосредственного участия субъекта – сюда можно отнести неверные настройки, избыточно открытые порты, запущенные службы, а также работу вредоносного ПО различных видов) и вследствие причин техногенного характера.

Таким образом, принимая во внимание ключевые критерии понятия «утечка информации» (несанкционированность и неконтролируемость), важнейшими элементами процесса защиты от утечек информации как специфического вида угроз являются следующие:

- Управление доступом к информации конфиденциального характера (принцип «правильная информация в правильных руках»).
- Защита информации от ознакомления недопущенным лицом (шифрование, технологии Digital Rights Management (DRM) и др.).
- Защита информации от неконтролируемого распространения и его пресечение, ключевым фактором здесь является точность и полнота выявления информации ограниченного доступа во внутренних и исходящих информационных потоках, серьезное влияние здесь могут оказать технологии искусственного интеллекта.
- Проработанные процедуры управления выявленными инцидентами утечек.
- Соблюдение правовых и этических норм при планировании воздействия на нарушителей требований информационной безопасности.

IV. Заключение

Как отмечено в работе [17] цифровая экономика формирует новые вызовы, которые требуют пересмотра «технологического» взгляда на решение проблем защиты конфиденциальности.

В настоящей статье предпринята попытка системного взгляда на научную организацию защиты информации от утечек, формирование базового понятийного аппарата и определение основных элементов программы, направленной на создание комплексной системы защиты.

Каждый из элементов такой программы нуждается в тщательной проработке и отдельном исследовании, при этом, по нашему мнению, исследованиям в области применения технологий искусственного интеллекта должно быть уделено особое внимание. Предлагаемая программа также подтверждает тезис о требовании междисциплинарности к профессиональной подготовке специалиста по информационной безопасности в цифровую эпоху.

Также следует признать, что уже на уровне методологии вопрос защиты от утечек недостаточно проработан – в отечественном законодательстве ответственность установлена только за утечки персональных данных, само понятие «утечка информации» не определено, а его статус в отношении разглашения (как правонарушения) не установлен.

Полагаем целесообразным включение понятия «утечка информации» как самостоятельного правонарушения, создающего предпосылки для совершения разглашения информации ограниченного доступа различных видов, в законодательные нормы, а до введения соответствующих поправок и доработок организациям, выстраивающим комплексную систему защиту информации, стоит предусмотреть необходимые положения в своих внутренних нормативных документах и договорах с третьими лицами.

Библиография

[1] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ : принят Государственной Думой 8 июля 2006 г. http://www.kremlin.ru/acts/bank/24157

[2] Зарубин А. В., Смирнов М. Б., Харитонов С. В., Денисов Д. В. Основные драйверы и тенденции развития DLP-систем в Российской Федерации // Прикладная информатика. – 2020. – Т. 15. – № 3. – С. 75-90. doi: https://doi.org/10.37791/2687-0649-2020-15-3-75-90

[3] Гарбузов Г. В., Теренин А. А., Бабак Н. Г. Использование технологий искусственного интеллекта в построении режима коммерческой тайны на предприятии // «Кибрарий», Сбербанк.

https://www.sberbank.ru/ru/person/kibrary/articles/tehnologiy_iskusstvennogo_intellekta_v_postroenii_rezhima_kommercheskoy_tayny
[4] Гарбузов Г. В., Теренин А. А. ИИ на страже банковских данных – 2: опыт «Сбербанка» // BIS JOURNAL. – 2020. – № 2. https://ib-bank.ru/bisjournal/post/1469
[5] Kim J., Lee C., Chang H. The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth // Sustainability. – 2020. – Vol. 12. – No. 24. Article number: 10639. doi: https://doi.org/10.3390/su122410639
[6] Добробаба М. Б. Проблема правового обеспечения защиты персональных данных при использовании технологий искусственного интеллекта // Устойчивое развитие России: правовое измерение : Сборник докладов X Московского юридического форума. – В 3-х частях, Университет имени О.Е. Кутафина (МГЮА), 06-08 апреля 2023 года. – М. : МГЮА, 2023. – С. 168-172. EDN: DABYFL
[7] Об утверждении Федерального стандарта бухгалтерского учета ФСБУ 14/2022 «Нематериальные активы» : приказ Минфина России от 30.05.2022 № 86н (Зарегистрировано в Минюсте России 28.06.2022 № 69031). https://www.consultant.ru/document/cons_doc_LAW_420322
[8] Об утверждении федерального стандарта оценки «Оценка интеллектуальной собственности и нематериальных активов (ФСО XI)» : приказ Минэкономразвития России от 30.11.2022 № 659. https://www.consultant.ru/law/hotdocs/78280.html
[9] Marriott Announces Starwood Guest Reservation Database Security Incident. Marriott News Center. 30 November, 2018. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident
[10] Marriott International, Inc. capitalization. All stocks today. 2023. https://www.allstockstoday.com/MAR-market-cap.html
[11] Cost of a Data Breach Report 2023. IBM Security, 2023. https://www.ibm.com/reports/data-breach
[12] 2023 Data Breach Report. Washington: Washington State Attorney General's office. https://newsletter.radensa.ru/wp-content/uploads/2023/12/DBR2023-FINAL.pdf
[13] 2023 Data Breach Investigations Report. Verizon, 2023. https://www.verizon.com/business/resources/reports/dbir
[14] Оценка ущерба вследствие утечек информации // Infowatch. 06 сентября 2023. https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii
[15] ГОСТ Р 50922-2006 Защита информации. Основные термины и определения : национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст: введен впервые: дата введения 2008-02-01 / подготовлен ФГУ «ГНИИИ ПТЗИ ФСТЭК России». М. : Стандартинформ, 2006.
[16] РС БР ИББС-2.9-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации» : рекомендации в области стандартизации Банка России : приняты и введены в действие Приказом Банка России от 11 апреля 2016 г. № ОД-1205.
[17] Швыряев П. С. Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. – 2022. – № 91. – С. 226-241. doi: https://doi.org/10.24412/2070-1381-2022-91-226-241
[18] Liu D., Liu X., Ma L., Chang Y., Wang R., Zhang H., Yu H., Wang E. Research on Leakage Prevention Technology of Sensitive Data based on Artificial Intelligence // 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC). – Beijing, China : IEEE Computer Society, 2020. – P. 142-145. doi: https://doi.org/10.1109/ICEIEC49280.2020.9152286
[19] Zhu T., Ye D., Wang W., Zhou W., Yu P.S. More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence // IEEE Transactions on Knowledge and Data Engineering. – 2022. – Vol. 34. – No. 6. – P. 2824-2843. doi: https://doi.org/10.1109/TKDE.2020.3014246
[20] Guha A., Samanta D., Banerjee A., Agarwal D. Deep Learning Model for Information Loss Prevention From Multi-Page Digital Documents // IEEE Access. – 2021. – Vol. 9. – P. 80451-80465. doi: https://doi.org/10.1109/ACCESS.2021.3084841

Problems of Definitions and Setting Goals for Data Leaks Protection

Georgy Garbuzov

***Abstract* - This article considers problematic methodological issues arising in the process of scientific organization of protection of restricted information from leakage and disclosure. In particular, it notes the lack of elaboration of terminology in the domestic legislation and its inconsistency in the sectoral legislation, which offers different, sometimes contradictory definitions. Problem statement: to determine the balance of approaches to the protection of restricted access information in the organization, to determine the criteria for the leakage of restricted access information as a specific type of threats to information security. Results: the authors conducted research to select the target approach to the definition of information leakage and its relationship with the disclosure of restricted information, in addition, the article defines approaches to the definition of objects of protection - restricted information - value and regulatory, as well as identified key aspects that should be taken into account in the future when developing a comprehensive system of protection of restricted information from leaks. Practical significance: the proposed approaches can be used by information security specialists of commercial and non-commercial organizations when building threat models of restricted access information and building systems of protection of restricted access information. Discussion: one of the directions of defining approaches to information leakage protection is presented, it is important to continue the synchronization of the conceptual apparatus in the domestic information security system.**

***Keywords* – restricted information, information leaks, information leakage protection, information disclosure, intangible asset, trade secret, Data Leak Protection, Data Leak Prevention, information protection.**

REFERENCES

[1] [On Information, Information Technologies and Information Protection: Federal Law No. 149-FZ of 27 July, 2006: Adopted by the State Duma on 8 July, 2006]. http://www.kremlin.ru/acts/bank/24157 (In Russ.)

[2] Zarubin A., Smirnov B., Kharitonov S., Denisov D., Main drivers and trends of DLP systems development in the Russian Federation. *Journal of Applied Informatics.* 2020. Vol. 15, no. 3. p. 75-90. (In Russ., abstract in Eng.) doi: https://doi.org/10.37791/2687-0649-2020-15-3-75-90

[3] Garbuzov G.V., Terenin A.A., Babak N.G. The usage of artificial intelligence technologies in an enterprise trade security policy creating. In: Kibrary, Sberbank. 2021 https://www.sberbank.ru/ru/person/kibrary/articles/tehnologiy_iskusstvennogo_intellekta_v_postroenii_rezhima_kommercheskoy_tayny (In Russ.)

[4] Garbuzov G.V., Terenin A.A. [Artificial Intelligence is on the guard of banking information-2: Experience of Sberbank]. BIS Journal. 2020. no. 2. https://ib-bank.ru/bisjournal/post/1469 (In Russ.)

[5] Kim J., Lee C., Chang H. The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth. Sustainability. 2020. Vol. 12, no. 24. Article number: 10639. doi: https://doi.org/10.3390/su122410639

[6] Dobrobaba M.B. Legal framework for personal data protection while using artificial intelligence technologies. In: Sinyukov V.N. (ed.) et. al. Proceedings of the X Moscow Legal Forum on Russia's Sustainable Development: Legal Environment. Part 1. M.: MSAL; 2023. p. 168-172. EDN: DABYFL (In Russ.)

[7] [On Approval of the Federal Accounting Standard FAS 14/2022 "Intangible Assets": Order of the Ministry of Finance of the Russian Federation No. 86n of 30 May 2022]. https://www.consultant.ru/document/cons_doc_LAW_420322 (In Russ.)

[8] [On approval of the federal valuation standard "Valuation of intellectual property and intangible assets (FSO XI)": Order of the Ministry of Economic Development of Russia No. 659 of 30 November, 2022]. https://www.consultant.ru/law/hotdocs/78280.html (In Russ.)

[9] Marriott Announces Starwood Guest Reservation Database Security Incident. Marriott News Center. 30 November, 2018. [Electronic resource]. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident

[10] Marriott International, Inc. capitalization. All stocks today. 2023. https://www.allstockstoday.com/MAR-market-cap.html

[11] Cost of a Data Breach Report 2023. IBM Security; 2023. https://www.ibm.com/reports/data-breach

[12] 2023 Data Breach Report. Washington: Washington State Attorney General's office. https://newsletter.radensa.ru/wp-content/uploads/2023/12/DBR2023-FINAL.pdf

[13] 2023 Data Breach Investigations Report. Verizon; 2023. Available at: https://www.verizon.com/business/resources/reports/dbir

[14] [Damage Assessment Due to Information Leaks]. Infowatch. 06 September, 2023. https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie -utechek-informatsii

[15] GOST R 50922-2006 Protection of information. Basic terms and definitions: National standard of the Russian Federation. The date it came into force 01.02.2008. Approved and enacted by Order of the Federal Agency for Technical Regulation and Metrology of December 27, 2006 No. 373-st.

[16] RS BR IBBS-2.9-2016 Ensuring information security of organizations of the banking system of the Russian Federation. Information Leakage Prevention' (adopted and put into effect by the Order of the Bank of Russia dated April 11, 2016 No. OD-1205). https://cbr.ru/statichtml/file/59420/rs-29-16.pdf

[17] Shvyriaev P.S. Data Breaches: The Main Enemy Within. E-journal "Public Administration". 2022. no. 91. p. 226-241. (In Russ., abstract in Eng.) doi: https://doi.org/10.24412/2070-1381-2022-91-226-241

[18] Liu D., Liu X., Ma L., Chang Y., Wang R., Zhang H., Yu H., Wang E. Research on Leakage Prevention Technology of Sensitive Data based on Artificial Intelligence. In: 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC). Beijing, China: IEEE Computer Society; 2020. p. 142-145. doi: https://doi.org/10.1109/ICEIEC49280.2020.9152286

[19] Zhu T., Ye D., Wang W., Zhou W., Yu P.S. More Than Privacy: Applying Differential Privacy in Key Areas of Artificial Intelligence. IEEE Transactions on Knowledge and Data Engineering. 2022. Vol. 34, no. 6. p. 2824-2843. doi: https://doi.org/10.1109/TKDE.2020.3014246

[20] Guha A., Samanta D., Banerjee A., Agarwal D. Deep Learning Model for Information Loss Prevention From Multi-Page Digital Documents. IEEE Access. 2021. vol. 9. p. 80451-80465. doi: https://doi.org/10.1109/ACCESS.2021.3084841

About the authors:

Georgy Garbuzov, Postgraduate student, Financial University under the Government of the Russian Federation, ORCID: http://orcid.org/0009-0008-7717-1488 (e-mail: g.garbuzov@mail.ru)