Технологии защиты нематериальных активов от атак на конфиденциальность

Г.В. Гарбузов

***Аннотация*— В статье рассматривается сущность понятия нематериального актива, его роли в современной экономике и важности защиты нематериальных активов от атак на конфиденциальность. В частности, рассмотрены свойства нематериальных активов, обуславливающие существование релевантных угроз информационной безопасности, не свойственных традиционным материальным активам. Также предложен подход к проведению анализа существующих технологий защиты нематериальных активов на основе жизненного цикла данных и проведен их сравнительный анализ. Постановка задачи: провести обзор существующих технологий защиты нематериальных активов и предложить методику выбора одной или нескольких технологий для применения на коммерческом предприятии. Результаты: оценена значимость нематериальных активов для коммерческого предприятия и подтверждена актуальность проблемы их надлежащей защиты, проведен обзор существующих технологий защиты для различных этапов жизненного цикла данных, обозначены актуальные проблемы в отдельных областях. Практическая значимость: предложенные подходы могут использоваться специалистами коммерческих и некоммерческих организаций при проектировании систем информационной безопасности, предназначенных для защиты нематериальных активов. Обсуждение: представлен подход к построению технологической системы защиты нематериальных активов, основанный на жизненном цикле данных.**

***Ключевые слова*— нематериальный актив, коммерческая тайна, ноу-хау, утечка информации, технологии защиты от утечек информации, жизненный цикл данных, DAMA, Data Leak Protection, защита информации.**

I. Нематериальные активы – сущность и роль в современной экономике

Нематериальный актив, т.е. актив, не имеющий вещественной формы [1], представляет особую ценность для любой современной организации. Коммерческая тайна [2] и интеллектуальная собственность [3], такие как рецептуры и технологии производства медицинских препаратов, описания изобретений и ноу-хау, стратегические планы развития, диверсификации бизнеса и его экспансии в другие отрасли и на другие территории, клиентские базы, имеются сегодня в каждой современной коммерческой организации. Они в состоянии обеспечить коммерческие преимущества их обладателям в условиях конкуренции, но только пока они надлежащим образом защищены.

Статья получена 26 июля 2024.

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

Информация, как разновидность нематериального актива, имеет ряд уникальных свойств (неисчерпаемость, возобновляемость, склонность к самокопированию и т.д.), обуславливающих её использование в качестве фактора производства или товара все более выгодным в условиях цифровой экономики, и, как следствие, формирующих устойчивый тренд на изменение в структуре активов современных предприятий, значительно снизив долю активов материальных. По данным аналитического агентства Ocean Tomo (Рис.1)[1], еще в 1975 году доля материальных активов компаний, входящих в рейтинг S&P500, составляла 83%, однако, в 1985 она была уже на уровне 68%, а в 1995 их доля снизилась до 32%.

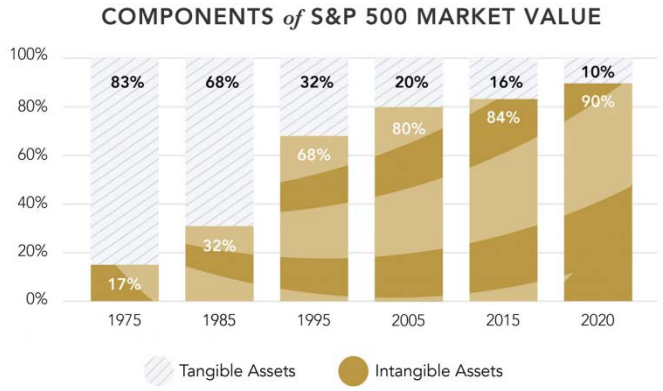

Рис. 1. Структура активов компаний S&P500

Сегодня 90% активов крупнейших компаний составляют именно нематериальные активы: патенты, ноу-хау, информация, составляющая коммерческую тайну, наборы и базы данных, программное обеспечение, бренды, торговые марки, результаты научно-исследовательских и опытно-конструкторских разработок. За последние полвека характер и технологии производства изменились столь радикально, что у многих современных компаний может вовсе не быть фабрик и оборудования, при этом они могут обладать рекордной даже по мировым меркам капитализацией, что особенно характерно для наукоемких отраслей, таких как ИТ. Так, реализация с 2011 года в Российской Федерации Стратегии инновационного развития привела к устойчивому росту затрат на НИОКР: по данным аналитики[2], за 10 лет (с 2010 по 2020 год) объем затрат

[1] Ocean Tomo. Intangible Asset Market Value Study, 2020. [Электронный ресурс]. URL: https://oceantomo.com/intangible-asset-market-value-study/

[2] Мазур Н. З., Попова А. В., Демьянец Е. А. Величина нематериальных активов предприятий РФ [Электронный ресурс] // Патентное бюро «ВКО-Интеллект», 2024. URL: https://www.vko-intellekt.ru/media-center/velichina-nematerialnyh-aktivov-predpriyatij-rossii/?ysclid=lvw126f8hy658728497

российских компаний на НИОКР, т.е. фактически, затрат на обладание нематериальными активами, выросло почти в 2,5 раза (Рис.2).

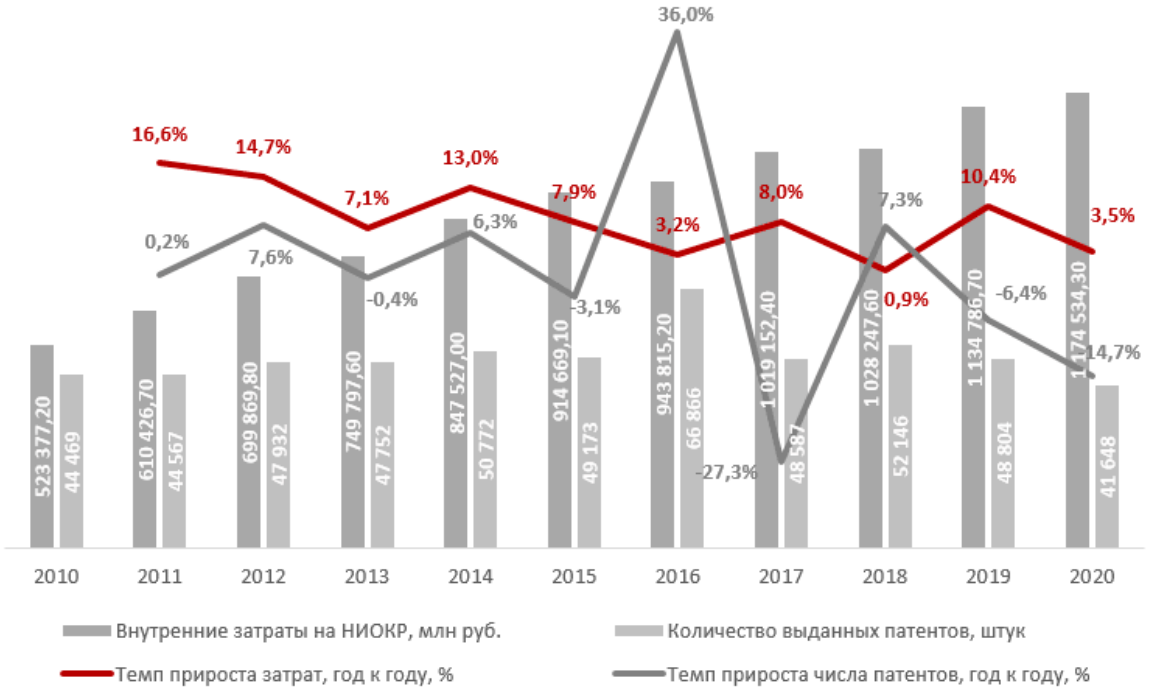

Рис. 2. Объемы затрат на НИОКР и патентования в РФ

Следует отметить, что по величине показателя доли нематериальных активов российские компании сегодня значительно уступают зарубежным и средняя доля нематериальных активов в балансе компаний РФ находится на уровне всего 4,1%. При этом самая значительная доля нематериальных активов (26,5%), у медиа-организаций, а у «наукоемких» отраслей – информационных технологий, научных исследований – этот показатель колеблется на уровне 4-5% (Рис.3).

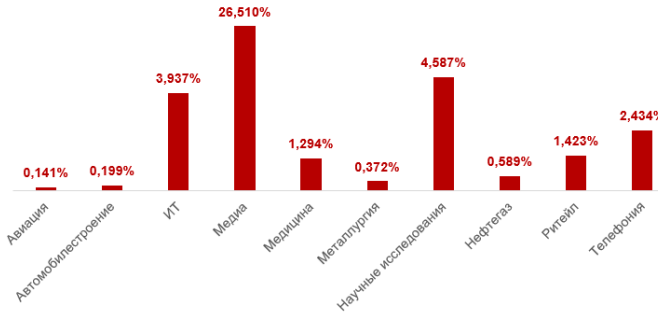

Рис. 3. Доля нематериальных активов по отраслям в РФ[3]

Тем не менее, с учетом мировых трендов, можно с уверенностью утверждать, что доля нематериальных активов в балансе как иностранных, так и отечественных предприятий будет неуклонно расти, а владение нематериальными активами будет играть все более значительную роль в их экономической устойчивости. Именно поэтому деловая среда и бизнес являются мощнейшим драйвером развития методов защиты нематериальных активов. Любой современной компании необходимо серьезно относиться к угрозам, представляемым нематериальным активам, учитывать их при проектировании систем защиты. А также принимать иные меры, включающие в себя как технические, так и организационные мероприятия, направленные на сохранение ценности нематериальных активов, в особенности, стоящих на балансе предприятия, и влияющих на его капитализацию.

II. Угрозы безопасности нематериальных активов

Говоря об угрозах безопасности нематериальных активов мы будем прежде всего иметь в виду те, что приводят к их обесцениванию и здесь следует обратить особое внимание на охрану коммерческой тайны и интеллектуальной собственности, которые имеются в каждой современной организации. Например, рецептуры и технологии производства медицинских препаратов, описания изобретений и ноу-хау, стратегические планы развития, диверсификации бизнеса и его экспансии в другие отрасли и на другие территории, клиентские базы [4], [5].

Указанные нематериальные активы могут утратить ценность в результате реализации целого спектра различных угроз[4]. Например, искажения или подмены содержания (атаки на целостность), утраты возможности использования актива или его части (атаки на доступность), несанкционированного доступа к активу со стороны конкурентов, с целью его последующего воспроизводства или принятия управленческих решений (атаки на конфиденциальность).

[3] Там же.

[4] Угрозы, объектом которых являются *права* в отношении нематериальных активов – патентные споры, оспаривание авторских прав и т.д. – в настоящей статье не рассматриваются.

Из перечисленных выше угроз внешних воздействий, в условиях конкурентной экономической среды, в которых действует коммерческое предприятие, одной из самых существенных следует принять угрозу конфиденциальности, поскольку последствия её реализации не только влечет применение к организации штрафов и причиняет ущерб владельцу нематериального актива (обладателю информации – коммерческой организации), но влияет и на других участников рынка, в том числе потребителей, которые не в состоянии реализовать свой спрос. Более того, нарушения конфиденциальности информации способны принести ущерб отрасли и даже рынку в целом, поскольку нематериальные активы, способные приносить прибыль, либо вовсе утрачивают такую способность, например, будучи открыто опубликованы, либо способствуют обогащению предприятий, вступивших во владение такими активами противозаконно, в результате *разглашения* информации ограниченного доступа, дискредитируя таким образом рыночные механизмы и правила честной конкуренции [6].

Реализацию угрозы конфиденциальности информации называют *утечкой* информации [7], которой мы будем считать несанкционированную и не контролируемую обладателем передачу (предоставление, распространение, доступ) конфиденциальной информации. Заметим, что утечка информации – это сам факт ее передачи, не включающий ознакомления с ней третьим лицом, при этом результатом утечки может стать ознакомление с ней третьим лицам без согласия обладателя или в нарушение условий договора, тогда можно говорить о разглашении, которое и станет непосредственной причиной обесценивания нематериального актива. В случае, если информация являлась критичным нематериальным активом (как, например, для наукоёмких производств, широко использующих объекты интеллектуальной собственности), это может не только привести к значительным финансовым потерям[5] [8], [9], но даже поставить предприятие на грань банкротств[6] [10]. При этом организации, столкнувшиеся с утечками информации, несут не только прямые финансовые издержки, но и значительный репутационный ущерб [11].

Описанные случаи далеко не единственные, согласно данным западных аналитических агентств [12-14] 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). Количество утечек конфиденциальной информации в 2022 в мире за год увеличилось более чем в 3 раза (с 1920 до 6856), а в России этот показатель вырос более чем вдвое[7]. В подавляющем большинстве случаев (82%) человеческий фактор – ошибки и халатность персонала, злоупотребление привилегиями, социальная инженерия – являются определяющими. Расходы на утечку с 2020 по 2022 год выросли на 13%, причем ужесточение законодательства в части ответственности за утечки информации, служит дополнительным негативным фактором, вынуждающим пострадавшие от утечек компании нести еще большие расходы. Согласно отчету Экспертно-аналитического центра ГК InfoWatch [8], количество утечек в 2023 году на 65% превысило показатели 2022 года, а объем утечек нематериальных активов (т.е. информации, стоящей на балансе предприятия и прямо влияющей на его капитализацию – интеллектуальной собственности, секретов производства, коммерческой тайны и пр.) в общем объеме утечек вырос почти втрое относительно того же периода, при этом больше всего утечкам подвержен промышленный сектор. В 70% случае утечки информации имели умышленный характер.

При проектировании системы защиты от утечек необходимо учитывать все источники возникновения угроз и все возможные каналы [15], [16]. Однако, говоря об утечках информации, с учетом современных реалий и имевших место громких инцидентов, в данной статье мы сосредоточимся на электронных каналах утечки информации, использующих телекоммуникационные каналы связи, не рассматривая каналы материальные и аудиовизуальные (сфотографировать или вынести на бумаге клиентскую базу в 1 миллион строк практически нереально). Кроме того, в данной статье мы будем рассматривать только меры защиты от утечек, имеющих внутреннюю антропогенную причину, т.е. возникших в результате действий работников организации. Понятно, что утечки информации, возникающие по причине неверной конфигурации оборудования или программного обеспечения, например, межсетевых экранов, а также из-за действия хакеров и вредоносных программ, должны предотвращаться специальными методами (регламентирование и стандартизация, тестирование на проникновение, регулярный аудит

[5] Примером может служить кража коммерческих секретов на 60 млн долларов США бывшим работником тайваньской компании HCM, являющейся поставщиком материалов для производства LMFP (литий-марганцево-железо-фосфатных батарей), в результате которой злоумышленник завладел 5681 файлом, в которых содержались данные о материалах, процессах, дизайне и разработке оборудования. См.: Wu J.-ch., Wu K.-h. Man indicted for stealing NT$2 billion worth of trade secrets [Электронный ресурс] // Focus Taiwan (CNA English News). July 15, 2024. URL: https://focustaiwan.tw/society/202407150020

[6] Например, банкротство Cambridge Analytica вследствие утечки данных из Facebook в 2018 или банкротство финской сети психотерапевтических центров Vastaamo в 2021 вследствие кражи сведений о сеансах психотерапии и персональных данных 40.000 пациентов. См.:

Cambridge Analytica closing after Facebook data harvesting scandal [Электронный ресурс] // The Guardian. May 2018. URL: https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say ;

Ralston W. They Told Their Therapists Everything. Hackers Leaked It All: A mental health startup built its business on easy-to-use technology. Patients joined in droves. Then came a catastrophic data breach [Электронный ресурс] // Wired. May 4, 2021. URL: https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/

[7] Аналитический отчет об оценке ущерба вследствие утечек информации [Электронный ресурс] // ЭАЦ ГК InfoWatch. 06 сентября 2023. URL: https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii

[8] Отчет об утечках информации в мире за последние два года [Электронный ресурс] // ЭАЦ ГК InfoWatch. 11 апреля 2024. URL: https://www.infowatch.ru/analytics/analitika/issledovaniye-utechek-informatsii-v-mire-za-posledniye-dva-goda

безопасности, выявление избыточных прав, остановка неиспользуемых служб и т.д.). Отсюда следует третье ограничение – в качестве мер защиты нематериальных активов мы будем рассматривать только технические меры, а меры организационного и правового характера, несомненно эффективные в ряде случаев, в данной статье не рассматриваются.

III. Технологии защиты нематериальных активов

За методологическую основу для выработки подхода к построению системы защиты имеет смысл взять жизненный цикл нематериального актива. Согласно [17] каждый этап жизненного цикла информации (данных) должен предусматривать использование защитных мер, начиная с момента создания информации и до её уничтожения. Рассмотрим подробнее жизненный цикл информации по DAMA[9]-DMBOK (Рис.4):

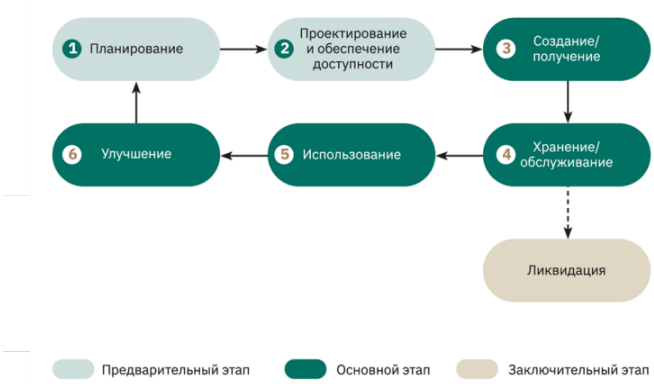

Рис. 4. Жизненный цикл информации DAMA-DMBOK

На рисунке 4 приведена общая последовательность этапов жизненного цикла информации, однако в конкретной коммерческой организации схема может быть уточнена – какие-то этапы могут отсутствовать или наоборот, могут быть расширены на несколько подэтапов. Объясняется это, прежде всего, тем, что информация в каждой конкретной организации от места возникновения до места уничтожения движется по своему индивидуальному пути и имеет различные источники *происхождения* (*lineage*) и для обеспечения надежной защиты этой информации необходимо инвентаризовать и учесть все источники происхождения информации всех видов (в том числе открытой информации), а также обеспечить контроль и учет за каждым перемещением информации из системы в систему или во внешний мир, где к информации предоставляется доступ и где она используются для ведения бизнеса. В этой связи идентификация *lineage* представляется важнейшим элементом, на котором базируется вся система защиты информации.

При построении контрольных процедур организация может столкнуться с большими трудностями, так как жизненный цикл информации с учетом её *lineage* может быть чрезвычайно запутанным и содержать массу пересечений, поэтому [17] обращает внимание на два важнейших принципа защиты информации, которые необходимо учесть:

– Создание и использование – важнейшие этапы жизненного цикла информации, на которые следует обратить внимание при построении системы управления информацией. Здесь необходимо исходить из принципа соразмерности ценности информации (причем не только с точки зрения стоимости нематериального актива, но и с позиций возможного применения штрафных санкций за нарушение внешних требований) и стоимости её защиты, в том числе от утечек. Следует также отметить, что в концепции жизненного цикла DMBOK использование информации включает её передачу/предоставление доступа к информации.

– При планировании защитных мер необходимо фокусироваться на критически важной информации, то есть уметь отделять её от прочей. Организация может создавать и хранить огромное количество информации различных видов, значительная часть которой не используется, или хуже, используется внутренними злоумышленниками в корыстных целях. При этом контролировать всю имеющуюся в распоряжении организации информацию одинаково эффективно невозможно или неоправданно дорого, а, значит, необходимо иметь а) **четкие критерии**, позволяющие отделить критически важную информацию от рядовой (излишней, устаревшей, тривиальной) и б) **технологии,** позволяющие выявить критически важную информацию в потоках данных и хранилищах.

Из этого следует вывод о том, что планирование и реализация мер по обеспечению защиты информации всегда должны начинаться с её классификации – определения видов и состава информации, имеющей наибольшее значение для организации, на основе характера взаимодействия этой информации с бизнес-процессами и её «вклада» в формирование прибыли коммерческой организации [18]. В общем случае, порядок проведения такой классификации и дальнейших необходимых шагов выглядит следующим образом:

1. Идентификация и классификация критичной информации. В зависимости от типа организации и отрасли бизнеса, она может обладать различной по объему, структуре и предъявляемым к ней требованиями информацией (например, персональными данными сотрудников, клиентов, пациентов, данными платежных карт, информацией, составляющей коммерческую тайну, объекты интеллектуальной собственности и др.).

2. Определение мест возникновения (создания), хранения и каналов передачи критичной информации. Результаты этой работы должны использоваться при ранжировании требований безопасности в зависимости от концентрации критичной информации в конкретном хранилище или канале её передачи.

3. Определение мер безопасности для каждого выявленного на предыдущем этапе хранилища информации или канала её передачи. Необходимые меры могут унифицироваться и группироваться в уровни (профили) защиты.

[9] DAMA (Data Management Association) International – основанная в 1980 г. в Лос-Анджелесе (США) и действующая с 1988 г. в статусе международной некоммерческой организации добровольная профессиональная ассоциация специалистов по управлению данными. DAMA International : сайт [Электронный ресурс]. URL: https://www.dama.org

4. Контроль соблюдения требований. Информационные системы и средства передачи информации должны осуществлять функции мониторинга, позволяющие фиксировать штатные события использования нематериального актива, так и выявлять нарушения требований безопасности (например, несанкционированный доступ к информации, повышение привилегий, нелегитимная передача информации третьему лицу). Для мониторинга порядка доступа и использования информации используются как средства пассивного мониторинга, позволяющего отслеживать изменения и отклонения системы от штатного состояния, так и активного, например, специализированных систем класса DLP (Data Leaks Prevention, Система предотвращения утечки) [19], способные не только информировать сотрудника безопасности о нарушении, но и прервать связанное с ним действие (например, передачу информации).

Таким образом, защита нематериальных активов коммерческого предприятия должна осуществляться как на этапе их создания (классификация информации, определение критичной информации), так и на этапе использования (включая предоставление доступа к информации и её передачу), с использованием различных методов и технологий, которые каждая организация выбирает самостоятельно исходя из модели угроз и множества других факторов, таких как стоимость нематериальных активов, зрелость процессов безопасности и стоимость защитных мер. Согласно некоторым исследованиям [20], выполненным на основе анализа публикаций об используемых методах защиты конфиденциальной информации в период с 2011 по 2022 год, самым популярным (используемым наибольшим количеством организаций) методом защиты конфиденциальной информации является шифрование (около 40%), а на втором месте использование технологий машинного обучения (около 12%), применяемых в дополнение в традиционным DLP технологиям. Таким образом, итоговый набор основных технологий, используемых для защиты нематериальных активов от угроз, связанных с атаками на конфиденциальность, с учетом подхода, основанного на жизненном цикле данных, предлагается объединить в три группы следующим образом:

1. Управление доступом. Реализует известный принцип безопасности «Need-To-Know» («правильная информация в правильных руках»). Включает в себя определение объекта доступа, субъекта доступа и правил доступа. Управление доступом может быть реализовано различными методами – избирательное управление доступом (Discretionary Access Control, DAC), ролевое управление доступом (Role-Based Access Control, RBAC), управление доступом на основе атрибутов (Attribute-Based Access Control, ABAC) и др. Определение объекта доступа невозможно без выполнения классификации критичных данных, поскольку именно от этого зависят правила разграничения доступа.

2. Шифрование информации. Процесс математического преобразования открытого текста в сложный код, который невозможно прочитать без ключа, который не может быть вычислен на основе других элементов зашифрованной информации. Существует четыре основных метода шифрования – хеширование, симметричное шифрование и асимметричное шифрование частным (закрытым) и публичным (открытым) ключом. Стоит отдельно упомянуть решения класса IRM (Information Rights Management), являющиеся подвидом систем управления цифровыми правами (DRM, Digital Rights Management) и реализующие гибкие механизмы управления и дистрибуции ключей шифрования для управления доступом к конкретному документу. Применение данного метода защиты также базируется на данных классификации информации и определения критичных объектов защиты.

3. Активный мониторинг. Защита информации от неконтролируемого распространения и её пресечение путем непрерывного контроля мест хранения информации и каналов её передачи (внутренних и внешних). Реализуется такая мера, как правило, с использованием систем класса DLP, осуществляющая выявление конкретных объектов защиты (нематериальных активов) в хранилищах данных и каналах передачи информации (WEB, электронная почта, съемные носители информации, печать и др.). Классификация данных также является критически важным элементом, необходимым для эффективного функционирования DLP системы, характеризующейся величинами точности (precision) и полноты (recall) рода, зависящих от величины ошибок первого (False Positive, FP) и второго (False Negative, FN) рода, и определяемых как:

$$precision = \frac{TP}{TP + FP}$$

$$recall = \frac{TP}{TP + FN}$$

Где TP – количество верно классифицированных объектов класса из общего числа элементов этого класса, FP – количество неверно классифицированных объектов класса из общего числа элементов другого класса, FN – количество неверно классифицированных объектов класса из общего числа элементов этого класса.

Для защиты нематериальных активов от атак на конфиденциальность могут использоваться все три группы технологий или их комбинации, объединенные в одном продукте, например системах класса DAG (Data Access Governance), реализующие несколько технологий для управления жизненным циклом информации, однако следует констатировать, что организация эффективного процесса защиты нематериальных активов от утечек, независимо от выбранных организацией технологий защиты, должна базироваться на а) результатах классификации информации и б) способности качественно её идентифицировать (обнаруживать) в файловых ресурсах или каналах связи.

Следовательно, **классификация информации является ключевым элементом при выстраивании эффективной системы защиты нематериальных**

активов, она в равной степени необходима как при установлении уровней конфиденциальности информации (разработка политик и правил классификации на основе вышеупомянутого «вклада» нематериального актива в прибыль организации, возможности наложения штрафных санкций за нарушение обязательных для соблюдения внешних требований), так и при непосредственной идентификации (выявлении) критичной информации, являющейся объектом защиты, в общем объеме хранимых или передаваемых данных для избирательного применения соответствующих технологий (мер) защиты. В случае игнорирования или некачественного выполнения классификации, критичная информация будет неверно идентифицирована, что в конечном итоге приведет либо к её утечке (недостаток контроля), либо к необоснованным усложнениям бизнес-процессов (избыток контроля), что в одинаковой степени может негативно отразиться на прибыли коммерческой организации или, в свете введения оборотных штрафов за утечку персональных данных, привести её к банкротству[10].

Следует отметить, что технологии идентификации классифицированной информации сегодня несовершенны и в подавляющем большинстве случаев классификация проводится либо человеком (владельцем нематериального актива – обладателем информации) либо при его непосредственном участии (верификации). И если те же DLP системы, работающие на основе статичных правил, демонстрируют приемлемые уровни точности (Precision) и полноты (Recall) при детектировании данных, представленных в табличной форме (структурированном виде), они демонстрируют чрезвычайно низкую эффективность при детектировании информации, представленной в неструктурированном виде – презентациях, текстовых офисных документах, сообщениях. И это может представлять серьезную проблему для организаций, значительная часть нематериальных активов которых представлена именно в неструктурированном виде – конструкторские бюро, высокотехнологичные производства, инновационные проекты, патентные подразделения и тому подобные.

IV. Заключение

Нематериальные активы играют все более возрастающую роль в современной цифровой экономике, а утрата ценности нематериального актива может причинить коммерческому предприятию значительный финансовый ущерб. Указанные нематериальные активы могут утратить ценность в результате различных угроз, но в условиях конкурентной экономической среды одной из самых существенных следует принять угрозу конфиденциальности, для защиты от которой предприятию необходимо создать систему защиты. В настоящей статье предложен подход к построению такой системы защиты на основе жизненного цикла данных, ключевыми элементами которой являются система классификации информации и технологии идентификации критичной информации в информационно-технологической инфраструктуре предприятия. Отмечено, что, технологии, реализованные в современных системах безопасности, хорошо справляются с детекцией и анализом структурированных данных, но для работы с неструктурированной информацией они недостаточно эффективны. Учитывая объемы неструктурированной информации, скорость её накопления и изменчивость, эти технологии нуждаются в дополнительной проработке с тем, чтобы позволять гибко и оперативно управлять политиками безопасности, направленными на предотвращение возможных утечек информации, с минимальным участием человека.

[10] Батыров Т. Малый бизнес предупредил о банкротствах из-за штрафов за утечку персональных данных [Электронный ресурс] // Forbes. 22 марта 2024. URL: https://www.forbes.ru/tekhnologii/508702-malyj-biznes-predupredil-o-bankrotstvah-iz-za-strafov-za-utecku-personal-nyh-dannyh?ysclid=lw4nybaymq44535893

Библиография

[1] 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). URL: https://www.consultant.ru/document/cons_doc_LAW_420322

[2] О коммерческой тайне : федер. закон от 29.07.2004 г. № 98-ФЗ (последняя редакция) : принят Государственной Думой 9 июля 2004 г. URL: https://www.consultant.ru/document/cons_doc_LAW_48699/

[3] Гражданский Кодекс РФ. Часть четвертая : федер. закон от 18 декабря 2006 г. № 230-ФЗ : принят Государственной Думой 24 ноября 2006 г. URL: https://www.consultant.ru/document/cons_doc_LAW_64629/

[4] Borky J.M., Bradley T.H., Protecting Information with Cybersecurity // Effective Model-Based Systems Engineering. – Cham: Springer, 2019. – P. 345-404. https://doi.org/10.1007/978-3-319-95669-5_10

[5] Moro-Viscont R. The Valuation of Intangible Assets: An Introduction // Artificial Intelligence Valuation. – Cham: Palgrave Macmillan, 2024. – Pp. 41-129. https://doi.org/10.1007/978-3-031-53622-9_2

[6] Geistfeld M.A. Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability // DePaul Law Review. – 2017. – Vol. 66, issue 2. – P. 385-412, 2017. URL: https://via.library.depaul.edu/law-review/vol66/iss2/4

[7] Гарбузов Г. В. Проблемы дефиниций и постановки целей защиты от утечек информации ограниченного доступа // International Journal of Open Information Technologies. – 2024. – Т. 12, № 5. – С. 185-191. – EDN: ZXVIYQ

[8] Trequattrini R., Lardo A., Cuozzo B., Manfredi S. Intangible assets management and digital transformation: evidence from intellectual property rightsintensive industries // Meditari Accountancy Research. – 2022. – Vol. 30, No. 4. – P. 989-1006. https://doi.org/10.1108/MEDAR-03-2021-1216

[9] Haber E., Zarsky T. Cybersecurity for Infrastructure: A Critical Analysis // Florida State University Law Review. – 2018. – Vol. 44. – P. 515-577. URL: https://ir.law.fsu.edu/lr/vol44/iss2/3

[10] Pană M.M., Titu A.M., Ungureanu A.M. Strategies for Protecting the Intellectual Capital in the Knowledge-Based Organizations // Proceedings on The XXVII-th International Conference of Inventics «INVENTICA 2023». Sciendo, 2023. https://doi.org/10.2478/9788367405201-007

[11] Nugraha Y., Martin A. Cybersecurity service level agreements: understanding government data confidentiality requirements // Journal of Cybersecurity. – 2022. – P. 1-19. https://doi.org/10.1093/cybsec/tyac004

[12] Cost of a Data Breach Report 2023. – IBM Security, 2023. URL: https://www.ibm.com/reports/data-breach

[13] 2023 Data Breach Report. – Washington State Attorney General's office, 2023. 15 p. URL: https://newsletter.radensa.ru/wp-content/uploads/2023/12/DBR2023-FINAL.pdf

[14] 2023 Data Breach Investigations Repor. – Verizon, 2023. URL: https://www.verizon.com/business/resources/reports/dbir

[15] Allahrakha N. Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age // Legal Issues in the Digital

Age. – 2023. – Vol. 4, No. 2. – P. 78-121. https://doi.org/10.17323/2713-2749.2023.2.78.121

[16] Admass W.S., Munaye Y.Y., Diro A.A. Cyber security: State of the art, challenges and future directions // Cyber Security and Applications. – 2024. – Vol. 2, Article number: 100031. https://doi.org/10.1016/j.csa.2023.100031

[17] DAMA-DMBOK : Свод знаний по управлению данными. Второе издание // Dama International [пер. с англ. Г. Агафонова]. – Москва : Олимп-Бизнес, 2020. – 828 с.

[18] Ferrara E. Determine The Business Value Of An Effective Security Program – Information Security Economics 101. – Forrester Research, Inc., October 2, 2012.

[19] 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

[20] Herrera Montano I., García Aranda J.J., Ramos Diaz J., et al. Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat // Cluster Computing. – 2022. – Vol. 25. – P. 4289-4302. https://doi.org/10.1007/s10586-022-03668-2

Technologies for Protecting Intangible Assets from Confidentiality Attacks

Georgy Garbuzov

***Abstract* - The article considers the essence of an intangible asset, its role in the modern economy, and the importance of protecting intangible assets from confidentiality attacks. In particular, the properties of intangible assets that determine the existence of relevant threats to information security that are not inherent in traditional tangible assets are considered. An approach to analyzing existing technologies for protecting intangible assets based on the data life cycle is also proposed and their comparative analysis is carried out. Statement of the problem: to review existing technologies for protecting intangible assets and to propose a methodology for selecting one or more technologies for use in a commercial enterprise. Results: the significance of intangible assets for a commercial enterprise is assessed and the relevance of the problem of their proper protection is confirmed, an overview of existing protection technologies for various stages of the data life cycle is conducted, and current issues in certain areas are identified. Practical significance: the proposed approaches can be used by specialists in commercial and non-profit organizations when designing information security systems to protect intangible assets. Discussion: An approach to building a technological system for protecting intangible assets based on the data life cycle is presented.**

***Keywords* – intangible asset, trade secret, know-how, information leakage, information leakage protection technologies, data life cycle, DAMA, Data Leak Protection, information protection**

REFERENCES

[1] [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 May 30, 2022]. [Online]. Available: https://www.consultant.ru/document/cons_doc_LAW_420322 (In Russ.)

[2] [On Commercial Secrecy (with The Amendments and Additions): Federal Law No. 98-FZ of July 29, 2004: Adopted by the State Duma on 9 July, 2004]. [Online]. Available: https://www.consultant.ru/document/cons_doc_LAW_48699 (In Russ.)

[3] Civil Code of the Russian Federation (Part Four, (with The Amendments and Additions): Federal Law No. 230-FZ of December 18, 2006: Adopted by the State Duma on November 24, 2006]. [Online]. Available: https://www.consultant.ru/document/cons_doc_LAW_64629/ (In Russ.)

[4] J.M. Borky, T.H. Bradley, "Protecting Information with Cybersecurity", *Effective Model-Based Systems Engineering*, Cham: Springer, pp. 345-404, 2019. https://doi.org/10.1007/978-3-319-95669-5_10

[5] R. Moro-Viscont, "The Valuation of Intangible Assets: An Introduction", *Artificial Intelligence Valuation*, Cham: Palgrave Macmillan, pp. 41-129, 2024 https://doi.org/10.1007/978-3-031-53622-9_2

[6] M. A. Geistfeld, "Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability", DePaul Law Review, vol. 66, issue 2, pp. 385-412, 2017. Available at: https://via.library.depaul.edu/law-review/vol66/iss2/4

[7] G. Garbuzov, "Problems of Definitions and Setting Goals for Data Leaks Protection", *International Journal of Open Information Technologies*, vol. 12, no. 5, pp. 185-191, 2024. EDN: ZXVIYQ (In Russ.)

[8] R. Trequattrini, A. Lardo, B. Cuozzo, S. Manfredi, "Intangible assets management and digital transformation: evidence from intellectual property rightsintensive industries", *Meditari Accountancy Research*, vol. 30, no. 4, pp. 989-1006, 2022. https://doi.org/10.1108/MEDAR-03-2021-1216

[9] E. Haber, T. Zarsky, "Cybersecurity for Infrastructure: A Critical Analysis", *Florida State University Law Review*, vol. 44, pp. 515-577, 2018. Available: https://ir.law.fsu.edu/lr/vol44/iss2/3

[10] M.M. Pană, A.M. Titu, A.M. Ungureanu, "Strategies for Protecting the Intellectual Capital in the Knowledge-Based Organizations", *Proceedings on The XXVII-th International Conference of Inventics "INVENTICA 2023"*, Sciendo, 2023. https://doi.org/10.2478/9788367405201-007

[11] Y. Nugraha, A. Martin, "Cybersecurity service level agreements: understanding government data confidentiality requirements", *Journal of Cybersecurity*, pp. 1-19, 2022. https://doi.org/10.1093/cybsec/tyac004

[12] "Cost of a Data Breach Report 2023", IBM Security, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[13] "2023 Data Breach Report", Washington State Attorney General's office, 2023. 15 p. [Online]. Available: https://newsletter.radensa.ru/wp-content/uploads/2023/12/DBR2023-FINAL.pdf

[14] "2023 Data Breach Investigations Report", Verizon, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir

[15] N. Allahrakha, "Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age", *Legal Issues in the Digital Age*, vol. 4, no. 2, pp. 78-121, 2023. https://doi.org/10.17323/2713-2749.2023.2.78.121

[16] W. S. Admass, Y. Y. Munaye, A. A. Diro, "Cyber security: State of the art, challenges and future directions", *Cyber Security and Applications*, vol. 2, article number: 100031, 2024. https://doi.org/10.1016/j.csa.2023.100031

[17] DAMA International, *Data Management Body Of Knowledge*, 2nd ed. Basking Ridge, New Jersey: Technics Publications, 2017. 588 p.

[18] E. Ferrara, *Determine The Business Value Of An Effective Security Program – Information Security Economics 101*, Forrester Research, Inc., October 2, 2012.

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

[20] I. Herrera Montano, J.J. García Aranda, J. Ramos Diaz, et al., "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat", *Cluster Computing*, vol. 25, pp. 4289-4302, 2022. https://doi.org/10.1007/s10586-022-03668-2

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)