Объективизированный показатель защищенности электронных информационных ресурсов инновационного предприятия

Objectived indicator of security of electronic information resources of an innovative enterprise

doi 10.26310/2071-3010.2021.269.3.010

Д. К. Щеглов,
к. т. н., доцент, АО «Конструкторское бюро специального машиностроения»
✉ _dk@bk.ru

А. Г. Сайбель,
д. т. н., доцент, профессор, Научно-образовательный центр
АО «СЗРЦ Концерна ВКО «Алмаз – Антей»
✉ saybel_ag@mail.ru

С. В. Баушев,
д. воен. н., профессор, начальник, Научно-образовательный центр
АО «СЗРЦ Концерна ВКО «Алмаз – Антей» – Обуховский завод»
✉ baushev_sv@rirt.ru

D. K. Shcheglov,
cand. sci. (eng.), associate professor,
JSC «Konstruktorskoe byuro specialnogo mashinostroeniya»

A. G. Saybel,
doctor sci. (tech.), docent, professor,
Scientific and educational center of JSC NWRC of «Almaz – Antey» air and space defence corporation»

S. V. Baushev,
doctor sci. (tech.), professor, the chief,
Scientific and educational center of JSC NWRC of «Almaz – Antey» air and space defence corporation» – Obuhovskiy zavod»

В статье проводится семантический анализ понятий «информационный ресурс» и «инновационное предприятие». Рассматривается подход к оценке защищенности цифровых активов инновационных предприятий (организаций, компаний) в условиях современной парадигмы цифровой экономики, и предлагается объективированный показатель защищенности информационных ресурсов.

The semantic analysis of the concepts of «information resource» and «innovative enterprise» is carried out. An approach to assessing the security of digital assets of innovative enterprises (organizations, companies) in the modern paradigm of the digital economy is considered and an objectified indicator of the security of information resources is proposed.

Ключевые слова: информационный ресурс, инновационное предприятие, информационная безопасность, защищенность, объективированный показатель.

Keywords: information resource, innovative enterprise, information security, security, objectified indicator.

Вечный вопрос русского интеллигента не «кто виноват?» и «что делать?», а «кто будет платить?».

Л. В. Шебаршин (1935-2012),
генерал-лейтенант КГБ СССР

В современных экономических и геополитических условиях значительно возросла конкуренция на рынке высокотехнологичной продукции. Предприятия (компании), выводящие на рынок свои товары и/или услуги позже конкурентов, почти не имеет шансов на их успешную реализацию. Поэтому внедрение цифровых технологий и инструментов цифровой трансформации становится для большинства высокотехнологичных предприятий обязательным условием устойчивого развития бизнеса.

Цифровая трансформация высокотехнологичных предприятий промышленности подразумевает, в частности, постепенный переход от традиционных способов проектирования и производства изделий на основе чертежей к более современным технологиям работы с информационными ресурсами (ИР), к которым относятся, прежде всего, цифровые прототипы изделий, цифровые двойники изделий и объектов производства, большие данные и т. д. [1].

Накопленные ИР по выполненным и текущим проектам образуют так называемые цифровые активы, которые непрерывно обновляются и используются в онлайн-режиме на всех этапах жизненного цикла выпускаемой продукции и предоставляемых услуг, в конечном итоге, увеличивая капитализацию инновационных предприятий.

С целью формирования объективизированного показателя защищенности ИР инновационного предприятия проведем семантический анализ понятий «информационный ресурс» и «инновационное предприятие».

Несмотря на широкое применение информационно-коммуникационных технологий во всех сферах жизнедеятельности человека, в настоящее время отсутствует строгое определение понятия «информационный ресурс», принятое научным сообществом. Существующие определения даются по формальным признакам, когда целевому термину ставятся в соответствие несколько других терминов («система», «информация», «данные», «ресурс», «документ» и т. д.) из того же пространства. Каждый из этих терминов должен тоже иметь свое определение. В результате формируется не-

которая замкнутая сеть ссылок терминов друг на друга, в которой возможно бесконечное множество вариантов определений и из которой непонятна семантическая ценность целевого термина «информационный ресурс» для конкретного субъекта информационного взаимодействия. Например, в Федеральном законе № 24-ФЗ от 20.02.1995 г. «Об информации, информатизации и защите информации» [2] под понятием «информационный ресурс» понимались отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а в новой редакции этого закона — № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» [3] — рассматриваемый термин вообще отсутствует. То есть, весь понятийный аппарат информационных технологий сводится к формам представления таких сущностей, как «данные» или «информация», являющихся объектами защиты.

Включение информации в состав ресурсов не снимает неопределенности понятия «информационный ресурс», поскольку в российской науке и практике отсутствует однозначный подход к тому, какую информацию считать ресурсом, а какую не считать.

Тем не менее, на уровне аппаратных средств, где осуществляется обработка так называемых двоичных ИР, терминология и правила работы с ними строго регламентируется международными стандартами, на базе которых создаются различные электронные устройства для массового использования.

Однако на более высоком уровне прикладного программного обеспечения вопрос о том, как должны быть представлены ИР в автоматизированных информационных системах (АИС) до сих пор не нашел общепринятого решения. Существует множество подходов и даже проектов стандартов по архитектуре представления информационных ресурсов в АИС (например, TOGAF от Open Group, DoDAF от Министерства обороны США, ISO 10303, ISO 15926, Zachman Framework, Federal Enterprise Architecture, EUP), но универсального определения и стандарта до сих пор не разработано, хотя он чрезвычайно востребован.

Очевидно, что отсутствие устоявшегося понятия «информационный ресурс» и стандартов его представления в АИС делает проблематичным разработку эффективной политики любого уровня (международного, государственного, отраслевого и т. д.) по их созданию и промышленной эксплуатации в интересах науки, техники, производства и управления. В контексте же настоящей статьи формирование показателя защищенности весьма затруднительно без четкого понимания того, что представляет собой объект защиты информации.

В общем случае ИР условно сконцентрированы в трех видах пространств: в физическом пространстве (в частности, в форме бумажных документов), в ментальном пространстве (мозг человека) и в информационном (машинном) пространстве. При этом операции с ИР (обработка, сборка, деление) осуществляется, как правило, при взаимодействии указанных видов пространств и находится в области известной проблемы создания «человеко-машинных» интерфейсов [4].

Разновидность ИР, создание и эксплуатация которых требует использования соответствующих программно-технических средств, будем называть электронными информационными ресурсами (ЭИР). При этом отметим, что в ГОСТ 33249-2015 «ИТ. Индивидуализированные адаптируемость и доступность в обучении, образовании и подготовке. Часть 3. Описание электронных ресурсов» вводится термин «электронный ресурс» [5], а в ГОСТ Р 7.0.94-2015 «СИБИД. Комплектование библиотеки документами. Термины и определения» [6] дополнительно к этому термину «цифровой ресурс». В профессиональной литературе наряду с понятием «электронный информационный ресурс» используются понятия «машиночитаемый информационный ресурс», «цифровой информационный ресурс», которые могут рассматриваться как условные синонимы.

Решение вопроса формирования понятия «электронный информационный ресурс» с учетом его представления в АИС частично находится в области объектно-ориентированного подхода. С учетом изложенного можно предложить следующее определение: ЭИР — это совокупность информационных объектов (или классов объектов) в АИС, имеющих определенный тип, определяющийся комплексом свойств в форме атрибутов и методов. При том между объектами (или классами объектов) в АИС и понятиями естественного языка всегда должно существовать взаимно-однозначное соответствие, традиционно определяемое как изоморфизм. Частным случаем ЭИР может являться электронный документ по ГОСТ 2.051-2013 «ЕСКД. Электронные документы. Общие положения» [7], либо по ГОСТ Р 7.0.95-2015 «СИБИД. Электронные документы. Основные виды, выходные сведения, технологические характеристики» [8].

Рассмотрим определения термина «инновационное предприятие». Например, согласно ГОСТ 31279-2004 «Инновационная деятельность. Термины и определения» [9]: инновационное предприятие — это предприятие (объединение предприятий), разрабатывающее, производящее и реализующее инновационные продукты и (или) продукцию или услуги. При этом к инновационно активным относятся предприятия, осуществляющие разработку и внедрение новой или усовершенствованной продукции, технологических процессов или иных видов инновационной деятельности. Базовые термины в области инноваций и инновационной деятельности в РФ определятся Федеральным законом № 127-ФЗ от 23.08.1996 г. «О науке и государственной научно-технической политике» [10].

Результатом инновационной деятельности является инновационный продукт. В международной практике термин «инновационный продукт», как правило, отождествляется с термином «инновация» (innovation). В соответствии с Руководством Осло (Oslo Manual) [11] из серии методических документов Семейства Фраскати (Frascati Family), инновации классифицируются по области их применения на технологические, маркетинговые, организационные и т. п. Технологические инновации, в свою очередь, подразделяются на процессные и продуктовые (новые

и усовершенствованные). Таким образом, международный термин «продуктовая инновация» (product innovation) соответствует российскому термину «инновационная продукция».

Основные положения Руководства Осло используются Росстатом при проведении статистических исследований в области науки и инноваций. При этом критерии отнесения товаров, работ, услуг к инновационной продукции, согласно п. 4 ст. 4 Федерального закона № 223-ФЗ от 18.08.2011 г. «О закупках товаров, работ, услуг отдельными видами юридических лиц» [12], устанавливают федеральные органы исполнительной власти, осуществляющие функции по нормативно-правовому регулированию в установленной сфере деятельности. В частности, такие критерии определены приказом Минпромторга РФ № 1618 от 01.11.2012 г. «Об утверждении критериев отнесения товаров, работ и услуг к инновационной продукции и (или) высокотехнологичной продукции...» [13].

Инновационные предприятия (организации, компании) в своей стратегии в первую очередь ориентируются на создание новых продуктов, в качестве которых могут выступать как товары, так и услуги, разновидностью которых являются сервисы. Непрерывный процесс вывода на рынок готовых к реализации инновационных продуктов, как правило, осуществляется одновременно с созданием новых.

В инновационных предприятиях (организациях, компаниях) создание инноваций является главным видом деятельности, тогда как в производственных организациях главным видом деятельности является изготовление и реализация продукции и/или услуг. При этом, согласно распоряжению Минэкономразвития РФ № ЗР-ОФ от 31.01.2011 г. «Об утверждении методических материалов по разработке программ инновационного развития...» [14], к инновационной относится любая деятельность, имеющая своей целью разработку и внедрение новых технологий, инновационных продуктов и услуг, соответствующих мировому уровню, модернизацию существующих технологий.

Важным аспектом инновационной деятельности является проведение маркетинговых исследований рынков сбыта и поиск новых потребителей, информационное обеспечение возможной конкурентной среды и потребительских свойств товаров конкурирующих организаций, поиск новаторских идей и решений, партнеров по внедрению и финансированию создания инновационной продукции.

В самом общем случае ЭИР инновационного предприятия можно условно разделить на базовые и оперативные, подразделяющиеся на внешние и внутренние.

Базовые ЭИР включают в себя информацию, как правило, не являющуюся результатом труда коллектива работников предприятия (например, нормативно-правовые и нормативно-технические документы).

Оперативные внутренние ЭИР, в свою очередь, подразделяются на:

- технологические — научно-технические характеристики производства предприятия, в том числе сведения о технологических процессах, принципах проектирования, технологической подготовки производства, опытной отработки, а также технологические секреты, больше известные как ноу-хау;
- управленческие — сведения о составе и структуре предприятия, его внутренней организации, сведения о моделях и методах управления. Управленческая информация дает представление о стратегии и тактике предприятия на рынке.

Оперативные внутренние ЭИР могут содержать в себе как общедоступную, так и конфиденциальную информацию. Общедоступная информация, эта та информация, на распространение и обращение с которой со стороны предприятия и вышестоящих органов управления не накладываются ограничения. Конфиденциальная информация, как правило, защищается предприятием и его вышестоящими органами, на распространение и обращение с ней накладываются жесткие организационные ограничения.

Очевидно, что значимая для коммерческого успеха конфиденциальная информация подлежит защите, поскольку представляет интерес для предприятий-конкурентов.

Известно, что стоимость продукта определяется его себестоимостью и потребительской востребованностью. При этом значимый объем рыночной потребительской ниши и уникальность продукта позволяют устанавливать на него монопольно высокую цену, обеспечивающую сверхприбыль.

Уникальность инновационного продукта или услуги определяется невозможностью или сложностью их повторения конкурентами, что обеспечивается следующими, принципиально различными, способами:

- юридическим — патентование и регистрация прав на созданные объекты интеллектуальной собственности (изобретения, полезные модели, промышленные образцы), а также регистрация программ для ЭВМ и баз данных. Впоследствии юридически защищенные права на знания и технологии могут продаваться и приобретаться в овеществленной (машины и производственное оборудование) или невещественной форме (патенты, лицензии, раскрытие ноу-хау и т. п.);
- технологическим — сокрытие информации о ноу-хау. В ряде случаев разработчики прорывных технических и технологических решений отказываются от патентования по причине невозможности всеобъемлющей защиты оригинальной идеи, которая может быть установлена при анализе описания и формулы изобретения;
- маркетинговым — создание спроса (в некотором роде «моды») на инновационную продукцию за счет активной рекламы и продвижения бренда. Потребители инновационного продукта ассоциируют его с конкретным брендом и не заинтересованы в приобретении продуктов-аналогов.

В современных условиях ведения хозяйственной деятельности ключевые технические решения реализуются, как правило, в виде мехатроных систем, а временные и финансовые затраты на реинжиниринг готового изделия могут быть сопоставимы с затратами на разработку нового. При этом разработка осуществляется с применением специализированных аппаратных и

программных средств, предназначенных для создания проектно-конструкторских ЭИР. К данному типу ЭИР относятся цифровые прототипы изделий, расчетные конечно-элементные модели, конструкторская документация в цифровой форме, иная сопроводительная информация об инновационном продукте. Именно поэтому инновационные предприятия уделяют особое внимание защите своих цифровых активов от утечки, несанкционированного доступа, уничтожения или модификации [15].

Система информационной безопасности инновационного предприятия должна обеспечивать целостность, конфиденциальность и доступность его цифровых активов.

Обеспечение надежной защиты цифровых активов (совокупности ЭИР) инновационного предприятия подразумевает, прежде всего, предотвращение рисков нарушения информационной безопасности, а не ликвидацию их последствий.

В современной цифровой парадигме обеспечение защиты кого-либо от потенциальных угроз — продуктивный путь к собственному благополучию. Многие фирмы оказывают услуги по защите информации. При этом результативность реализуемых ими организационно-технических мероприятий сложно оценить количественно, что не позволяет выполнять научно-обоснованный сравнительный анализ альтернативных рекламных предложений.

В истории человечества можно назвать многочисленные варианты организации защиты чего-либо. Близким к теоретическому идеалу можно считать систему оказания охранных услуг, созданную в древней Японии, история которой продемонстрировала возможность существования на компактной территории значительных человеческих масс.

Обеспечение питанием своих семей и соплеменников для японцев стало возможным благодаря рисовой культуре, способной давать обильный урожай на небольших специфически организованных плодородных площадях. Недостатком рисового производства являются высокие требования к участкам, на которых осуществляется выращивание. Невозможность быстрого создания нового поселения, способного обеспечить пищей своих жителей, потребовала формирования системы защиты урожая от «непрошеных гостей». Частная армия, состоящая из освобожденных от сельскохозяйственных работ воинов, была предназначена для сохранения рисового урожая. Но сами воины также являются потребителями риса. Очевидное противоречие породило в японской культуре уникальный слой общества — самураев. Воин-одиночка, посвящающий все свое время подготовке к вооруженному противостоянию, или немногочисленная группа таких воинов, нанимались в качестве охраны к владельцу рисовых чек для обеспечения их безопасности. Малочисленность охраны определила специфику боевой подготовки самураев — для борьбы с многочисленными врагами воин должен обеспечивать свою победу минимальным числом результативных ударов при максимальном сохранении сил для длительного продолжения противостояния. При этом наносимые удары должны минимизировать риски повреждения оружия.

Уверенность в том, что самурай не сбежит при угрозе гибели, базировалась на понимании последствий такого поступка: несоблюдение кодекса чести карается неминуемой смертью от рук представителя ремесла, а участие в битве даже с превосходящим противником оставляет шансы на выживание.

Неотъемлемым условием возможности рассмотренного распределения общественных ролей является обладание самураями понятием чести и неукоснительного следования ее канонам.

Очевидно, что затраты на охрану не могут превышать потенциальный размер парируемого ущерба. При этом способность охраны выполнить свои функции является потенциальной.

Для спокойствия нанимателя наилучший вариант состоит в регулярном нападении врагов и успешном отражении атак охраной, верифицирующий уровень ее достаточности. Для охраны идеальным является вариант, при котором враги не нападают.

Совмещением обоих вариантов является ситуация, в которой охрана инициирует имитацию нападений, а наниматель воспринимает спектакль за реальность.

Разновидностью такой ситуации является рэкет, когда оплата безопасности осуществляется представителям организованных преступных групп (ОПГ) за гарантии отсутствия необходимости плат представителям других ОПГ. При этом различные ОПГ находятся в соглашении о территориальном разделении зон контроля. Подтверждением серьезности намерений являются периодические акции устрашения, направленные на формирование страха жесткого возмездия за непослушание.

В современном мире мы сталкиваемся со схожим положением вещей в сфере информационной безопасности. О существовании угроз информационной безопасности владельцы ЭИР узнают от организационных структур (коллективов штатных и/или привлекаемых специалистов), обеспечивающих эту безопасность. Угрозы информационной безопасности создаются (реализуются) представителями других организационных структур либо физическими лицами (хакерами, скрипт-киддирами). Соизмерить размер реальности угроз с затрачиваемыми на обеспечение информационной безопасности средствами владельцы ЭИР могут только на основании принимаемых на веру оценок, формируемых специалистами. При этом обеспечивающие информационную безопасность специалисты, в отличие от самураев, не несут ответственности за отсутствие методов защиты от новых угроз.

В несколько измененном виде схожая ситуация наблюдается при обеспечении защиты ЭИР, формирующихся в АИС инновационного предприятия на протяжении всего жизненного цикла инновационной продукции. Наиболее ценная первичная консолидированная информация о продукции содержится в АИС, предназначенных для выполнения проектно-конструкторских работ (моделирование, проектирование, управление инженерными данными и проектами).

Априорная неопределенность потенциального объекта исследования предъявляет к аппаратным и программным средствам, применяемым для выполнения

проектно-конструкторских работ, специфические требования универсальности, состоящие в необходимости их пригодности для исследования и разработки любых сложных технических систем, содержащих в своем составе какую-либо компьютерную информацию. Особенно ярко данная проблемная ситуация проявляется в отношении программного обеспечения.

Особенностью ЭИР, включающего программное и информационное обеспечение, является сложная взаимосвязь между его ценой и стоимостью. Целью разработки ИР является получение прибыли. На формирование ИР тратится средств больше, чем он стоит, что обусловлено потерями на проверку непродуктивных гипотез и другие поисковые исследования. Следовательно, цена ИР не превышает потенциальную прибыль.

Если цена хищения ЭИР не превышает его стоимость, то норма прибыли у конкурента разработчика ИР окажется выше, чем у правообладателя.

Следовательно, необходимо стремиться к обеспечению условия: цена кражи выше себестоимости ЭИР. С формальной точки зрения такое условие достижимо на одном из двух направлений: либо ЭИР представляет собой слабо формализованную распределенную структуру, хищение которой возможно только частично или избыточно, либо доступ к ИР является технически и технологически сложной процедурой с налаженной системой контроля доступа.

На каждом из обозначенных направлений решения поставленной задачи существует ограничение, связанное с необходимостью использования ЭИР в процессе создания инновационного продукта.

Исходя из представленных выше логических рассуждений следует, что наиболее эффективный способ получения доступа к ЭИР предприятия — через его работников. Этот простой вывод подтверждается данными «Лаборатории Касперского» о том, что 52% юридических лиц по всему миру считают своих сотрудников наибольшей угрозой системе корпоративной безопасности [16]. Согласно исследованию, проведенному компанией ESET, около 20% из 750 опрошенных респондентов хотя бы раз в жизни копировали рабочие материалы (базы клиентов, отчеты, планы и т. д.), чтобы впоследствии использовать их на новой работе или перепродать, а 7% рассказали, что даже после увольнения из компании они могли заходить на корпоративные порталы или рабочую почту удаленно [17].

Для количественного оценивания степени защищенности ЭИР предлагается использовать вероятность покрытия случайных множеств, как показатель текущей защищенности ЭИР в АИС [18].

При сдаче в эксплуатацию распределенной АИС справедливо полагать, что в ней отсутствуют известные уязвимости, что достигается их устранением в процессе проектирования и реализации АИС. Однако с течением времени неизбежно обнаруживаются новые уязвимости и безопасность АИС снижается [19].

Одним из известных путей поддержания АИС в защищенном состоянии является ее тестирование программно-аппаратными средствами на выявление ошибок и уязвимостей, а также на подверженность со стороны опубликованных или обнаруженных уязвимостей в других АИС.

Научный и практический интерес представляет собой проблема оценивания текущей защищенности эксплуатируемой АИС [20]. В качестве показателя текущей защищенности АИС предлагается использовать вероятность события, что злоумышленник нашел уязвимость ранее того момента, как это же самое в процессе тестирования эксплуатируемой АИС сделал ее разработчик (администратор) и устранил.

В такой трактовке можно сформулировать следующую математическую постановку задачи текущего оценивания защищенности АИС. Пусть все возможные уязвимости рассматриваемой АИС образуют некоторое множество A. Так как априори уязвимости неизвестны, более того, даже после окончания эксплуатации АИС могут существовать необнаруженные (неиспользованные) уязвимости, то множество A следует полагать случайным, т. е. $A_{\text{сл}\{W\text{сл}\}}$, в котором случайными будут являться как мощность $W_{\text{сл}}$ множества уязвимостей, так и набор составляющих его событий a_i, i=1, ..., $W_{\text{сл}}$.

Для нарушителя информационной безопасности АИС, как и для ее администрации, множество $A_{\text{сл}\{W\text{сл}\}}$ тождественно. Однако в процессе его наполнения во времени найденными уязвимостями со стороны злоумышленника и администрации следует полагать различными — в силу несовпадения используемого инструментария поиска обе стороны будут находить не обязательно одинаковые уязвимости, во-первых, и с различными интенсивностями, во-вторых. То есть, в процессе поиска уязвимостей злоумышленник и администрация получают различные текущие приближения (оценки) множества A, обозначим их $A_{\text{оц зл}}$ и $A_{\text{оц адм}}$, соответственно. Тогда вероятность того, что к моменту времени T множество $A_{\text{оц адм}}$ выявленных администрацией АИС уязвимостей покрывает подобное множество $A_{\text{оц зл}}$, т. е. $A_{\text{оц зл}}$ принадлежит $A_{\text{оц адм}}$, можно полагать вероятностью того, что АИС пребывает в защищенном состоянии:

$$P_{\text{защ}}(T) = P(A_{\text{оц зл}} \in A_{\text{оц адм}}; T).$$

Обозначим через $\lambda_{\text{зл}}$ и $\lambda_{\text{адм}}$ и зададим интенсивности обнаружения уязвимостей злоумышленником и администрацией АИС соответственно, при этом должно быть $\lambda_{\text{зл}} \leq \lambda_{\text{адм}}$, т. е. интенсивность обнаружения уязвимостей администрацией АИС выше, чем у злоумышленника. Теперь можно оценить наполнение множеств $A_{\text{оц зл}}$ и $A_{\text{оц адм}}$ к текущему моменту времени T. Зададим также и верхнюю границу мощности и формально сформируем множество $A_{\text{сл}}$ уязвимостей как множество случайных событий a_i, i=1, ..., $W_{\text{сл}}$; $W_{\text{сл}} < W_{\text{в.гр.}}$.

Применение методов теории вероятностей на практике часто затруднено необходимостью обоснования закона распределения случайной величины. В рассматриваемой задаче события a_i обнаружения уязвимостей злоумышленником и администрацией АИС носят внезапный характер, а режим эксплуатации АИС и поиска уязвимостей, как правило, является установившимся. В той связи можно принять допу-

щение, что интенсивности обнаружения уязвимостей $\lambda_{зл}$ и $\lambda_{адм}$ стремятся к некой постоянной величине. Тогда можно принять экспоненциальный закон распределения вероятности пребывания АИС в защищенном состоянии:

$$P_{защ}(t) = P_{защ}(T \leq t) = (1 - \exp(-\lambda_{адм} t)) \exp(-\lambda_{зл} t),$$

где t — время.

Как видно из приведенного выше соотношения вероятность пребывания АИС в защищенном состоянии представляет собой произведение вероятностей обнаружения уязвимости администрацией АИС и не обнаружения уязвимости злоумышленником.

В результате оказывается возможным путем имитационного моделирования или аналитически получить текущие оценки защищенности АИС. С течением времени множества $A_{оц\,зл}$ и $A_{оц\,адм}$ должны стать тождественными друг другу и исходному множеству A. Однако, такое возможно в процессе крайне длительной эксплуатации АИС, что как правило не наступает, так как АИС переживает свое развитие и появляется в новой версии — с новыми возможностями и новым множеством уязвимостей $A_{сл\{Wсл\}}$, диалектически повторяя очередной виток своего развития.

Представленный подход к оцениванию потенциальной защищенности цифровых активов, составляющих содержание уникальности инновационного продукта произвольного вида, позволяет формировать количественные риск-ориентированные оценки сроков сохранения конкурентоспособности выводимого на рынок продукта с учетом информационной защищенности результатов разработки. Кроме того, предложенный подход позволяет обоснованно распределять страховые риски инновационного предприятия-разработчика и фирмы, оказывающей услуги по реализации организационно-технических мероприятий по защите АИС.

Список использованных источников

1. Д. К. Щеглов, Н. А. Пиликов, В. И. Тимофеев. Концептуальные основы цифровой трансформации организации оборонно-промышленного комплекса// Автоматизация в промышленности. № 2. 2021. С. 15-25.
2. Федеральный закон № 24-ФЗ от 20.02.1995 г. «Об информации, информатизации и защите информации». Интернет. КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_5887.
3. Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и защите информации». Интернет. КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_61798.
4. В. Ю. Алексеева, Н. А. Пиликов, Д. К. Щеглов. Некоторые перспективные направления развития информационного обеспечения жизненного цикла сложных технических систем//Инновации. № 2 (196). 2015. С. 116-120.
5. ГОСТ 33249-2015 «Информационная технология. Индивидуализированные адаптируемость и доступность в обучении, образовании и подготовке. Часть 3. Описание электронных ресурсов» вводится термин «электронный ресурс». Интернет. Техэксперт. http://docs.cntd.ru/document/1200106860.
6. ГОСТ Р 7.0.94-2015 «Система стандартов по информации, библиотечному и издательскому делу. Комплектование библиотеки документами. Термины и определения». Интернет. Техэксперт. http://docs.cntd.ru/document/1200127747.
7. ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения». Интернет. Техэксперт. http://docs.cntd.ru/document/1200106860.
8. ГОСТ Р 7.0.95-2015 «Система стандартов по информации, библиотечному и издательскому делу. Электронные документы. Основные виды, выходные сведения, технологические характеристики». Интернет. Техэксперт. http://docs.cntd.ru/document/1200128317.
9. ГОСТ 31279-2004 «Инновационная деятельность. Термины и определения». Минск: Госстандарт Республики Беларусь, 2005. Впервые. Введ. 2005-09-01. 20 с.
10. Федеральный закон № 127-ФЗ от 23.08.1996 г. «О науке и государственной научно-технической политике». Интернет. КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_11507.
11. Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data.3rd edition. Paris: OECD/Eurostat, 2005. Руководство Осло: Рекомендации по сбору и анализу данных по инновациям. Третье издание. Совместная публикация ОЭСР и Евростата. Перевод на русский язык, издание второе исправленное. Москва, 2010.
12. Федеральный закон «О закупках товаров, работ, услуг отдельными видами юридических лиц» № 223-ФЗ от 18.08.2011 г. Интернет. КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_116964.
13. Приказ Минпромторга России № 1618 от 01.11.2012 г. «Об утверждении критериев отнесения товаров, работ и услуг к инновационной продукции и (или) высокотехнологичной продукции по отраслям, относящимся к установленной сфере деятельности Министерства промышленности и торговли Российской Федерации» (зарегистрировано в Минюсте России 11.03.2013 г. № 27584). Интернет. КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_143576.
14. Распоряжение Минэкономразвития РФ № ЗР-ОФ от 31.01.2011 г. «Об утверждении методических материалов по разработке программ инновационного развития акционерных обществ с государственным участием, государственных корпораций и федеральных государственных унитарных предприятий». Интернет. КонсультантПлюс. http://www.consultant.ru/cons/CGI/online.cgi?req=doc&base= EXP&n=510106&dst=100165#03863794503161948.
15. Л. Г. Данилова, М. Н. Охочинский, Д. К. Щеглов. Методология построения системы защиты данных в едином информационном пространстве корпорации//В сб. трудов XV Всероссийской НПК «Актуальные проблемы защиты и безопасности». Технические средства противодействия терроризму. Т. 2. СПб.: 2012. С. 70-75.
16. И. Носатов. Дураки и воры: свои сотрудники стали опаснее хакеров. https://iz.ru/1000295/ivan-nosatov/duraki-i-vory-svoi-sotrudniki-stali-opasnee-khakerov.
17. П. Юдина. Какие ошибки совершают компании в борьбе с воровством данных. https://www.vedomosti.ru/management/articles/2017/10/10/737221-oshibki-v-borbe-s-vorovstvom.
18. С. В. Баушев. Вероятность покрытия случайных множеств как показатель текущей защищенности информационных систем. Региональная информатика (РИ-2012). СПб.: СПОИСУ, 2012. С. 81.
19. Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику: учеб. пособие/Под ред. С. В. Баушева, А. С. Кузьмина. СПб.: БХВ-Петербург, 2016. 304 с.
20. О. А. Атакищев, И. С. Захаров, А. Г. Сайбель. Основные показатели результативности процесса функционирования измерительной системы с переменными параметрами элементов//Телекоммуникации. № 7. 2004. С. 2-5.

References

1. D. K. Shcheglov, N. A. Pilikov, V. I. Timofeev. Conceptual foundations of the digital transformation of the organization of the military-industrial complex//Automation in Industry. № 2. 2021. P. 15-25.
2. Federal Law «On Information, Informatization and Information Protection» dated 20.02.1995, № 24-FZ. Internet. ConsultantPlus. http://www.consultant.ru/ document/cons_doc_LAW_5887.
3. Federal Law «On Information, Information Technologies and Information Protection» dated July 27, 2006, № 149-FZ. Internet. ConsultantPlus. http://www.consultant.ru/ document/cons_doc_LAW_61798.
4. V. Yu. Alekseeva, N. A. Pilikov, D. K. Shcheglov. Some promising directions for the development of information support for the life cycle of complex technical systems// Innovations. № 2 (196). 2015. P. 116-120.
5. GOST 33249-2015 «Information technology. Individualized adaptability and accessibility in teaching, education and training. Part 3. Description of electronic resources «introduces the term» electronic resource». Internet. Techexpert. http://docs.cntd.ru/ document/1200106860.
6. GOST R 7.0.94-2015 «System of standards for information, librarianship and publishing. Acquisition of the library with documents. Terms and definitions». Internet. Techexpert. http://docs.cntd.ru/document/1200127747.

7. GOST 2.051-2013 «Unified system for design documentation. Electronic documents. General Provisions». Internet. Techexpert. http://docs.cntd.ru/document/1200106860.
8. GOST R 7.0.95-2015 «System of standards for information, librarianship and publishing. Electronic documents. Main types, imprint, technological characteristics». Internet. Techexpert. http://docs.cntd.ru/document/1200128317.
9. GOST 31279-2004 «Innovation activity. Terms and definitions». Minsk: Gosstandart of the Republic of Belarus, 2005. For the first time. Enter. 2005-09-01. 20 p.
10. Federal Law «On Science and State Scientific and Technical Policy» dated 23.08.1996, № 127-FZ. Internet. ConsultantPlus. http://www.consultant.ru/document/ cons_doc_LAW_11507.
11. Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data. 3rd edition. Paris: OECD/Eurostat, 2005. Oslo Handbook: Guidelines for the collection and analysis of innovation data. Third edition. Joint publication by OECD and Eurostat. Translation into Russian, revised second edition. Moscow, 2010.
12. Federal Law «On the procurement of goods, works, services by certain types of legal entities» dated 18.08.2011 № 223-FZ. Internet. ConsultantPlus. http://www.consultant.ru/document/cons_doc_LAW_116964.
13. Order of the Ministry of Industry and Trade of Russia dated 01.11.2012 № 1618 «On approval of the criteria for classifying goods, works and services as innovative products and (or) high-tech products by industries related to the established scope of activities of the Ministry of Industry and Trade of the Russian Federation» (Registered with the Ministry of Justice of Russia 11.03.2013 № 27584). Internet. ConsultantPlus. http://www.consultant.ru/document/cons_doc_LAW_143576.
14. Order of the Ministry of Economic Development of the Russian Federation of 31.01.2011 No. 3R-OF «On approval of methodological materials for the development of programs for innovative development of joint-stock companies with state participation, state corporations and federal state unitary enterprises». Internet. ConsultantPlus. http://www.consultant.ru/cons/CGI/online.cgi?req=doc&base=EXP&n=510106&dst=100165#03863794503161948.
15. L. G. Danilova, M. N. Okhochinsky, D. K. Shcheglov. Methodology for constructing a data protection system in a single information space of a corporation//In collection. Proceedings of the XV All-Russian NPK «Actual problems of protection and security». Technical means of countering terrorism. Vol. 2. SPb.: 2012. P. 70-75.
16. I. Nosatov. Fools and thieves: their employees have become more dangerous than hackers. https://iz.ru/1000295/ivan-nosatov/duraki-i-vory-svoi-sotrudniki-stali-opasnee-khakerov.
17. P. Yudina. What mistakes companies make in the fight against data theft. https://www.vedomosti.ru/management/articles/2017/10/10/737221-oshibki-v-borbe-s-vorovstvom.
18. S. V. Baushev. The probability of covering random sets as an indicator of the current security of information systems. Regional informatics (RI-2012). SPb.: SPOISU, 2012. P. 81.
19. Certification automated information systems and tools. Introduction to theory and practice: textbook. allowance/Ed. S. V. Baushev, A. S. Kuzmin. SPb.: BHV-Petersburg, 2016. 304 p.
20. O. A. Atakischev, I. S. Zakharov, A. G. Saybel. The main indicators of the effectiveness of the process of functioning of the measuring system with variable parameters of elements//Telecommunications. № 7. 2004. P. 2-5.