ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ЭКОНОМИЧЕСКИХ СУБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ СРЕДСТВ ЗАЩИТЫ

*Миронова Наталья Геннадьевна,
к. филос. н., доцент каф.*

*Управления информационной безопасности
ФГБОУ ВО Башкирский государственный университет,
Институт истории и государственного управления (Уфа)*

*Мифтахова Лиана Ильясевна
(студент)*

*ФГБОУ ВО Башкирский государственный университет,
Институт истории и государственного управления (Уфа)*

ENSURING THE SECURITY OF CONFIDENTIAL INFORMATION OF ECONOMIC SUBJECTS USING INTELLIGENT PROTECTIVE MEASURES

*Mironova Natalia Gennadievna,
Candidate of Philosophy,*

*Associate Professor of the Department.
Information Security Directorate
Bashkir State University (Ufa)*

*Liana Miftakhova (student)
Bashkir State University (Ufa)*

Аннотация. Рассматривается проблематика обеспечения информационной безопасности конфиденциальной информации с использованием интеллектуальных средств защиты.

Abstract. The problems of ensuring information security of confidential information using intellectual means of protection are considered.

Ключевые слова: информационная безопасность, защита информации, угроза утечки данных, нейросетевые модели.

Keywords: information security, information protection, the threat of data leakage, neural network models

Современная экономика насыщена цифровизацией и автоматизацией, в т.ч. интеллектуальной. Как и за рубежом, в России реализуются проекты по внедрению искусственного интеллекта в государственное управление, в работу ФНС, ФОМС, Росмолодежи, Минздрава, МВД, МЧС, Минтранса, Минсельхоза, Минпромторга и т.д. ([1], [2]). Активно внедряется интеллектуальная автоматизация в бизнес-структурах. Одна из сфер автоматизации – информационная безопасность информационной среды компаний, предприятий, учреждений, ЦОДов. Без защиты информации представить современную информационную инфраструктуру уже невозможно, и вопросы, связанные с организацией защиты государственной и служебной, профессиональной тайны, критически важной информации автоматизированных систем управления производственными процессами, автоматизации управления социальными, техническими, военными объектами приобретают критическое значение в современной обстановки оцифровки всего и вся.

Проблематика защиты информации опосредует принятие решений в бизнесе и государственном управлении, все в большей мере проникает в быденную жизнь граждан. Чем больше сведений о людях и процессах собирается, отчуждается в оцифрованном виде различными субъектами, становится средством и источником принятия разнообразных решений, тем большее значение приобретают меры информационной безопасности. Угрозы утечки информации ограниченного характера оборачивается прямым ущербом для бизнеса и граждан, утратой доверия к структурам, которые иницируют и осуществляют сбор, хранение, использование оцифрованных сведений о социальной и деловой жизни, создавая широкомасштабные экономические и политические риски для страны в целом. Злоумышленники, завладев ценной информацией, могут нанести урон репутации граждан, получить доступ к банковским счетам, к частной жизни, к государственным секретам.

Прямые каналы утечки информации – это целенаправленно осуществляемое несанкционированное получение защищаемых данных путем взлома систем защиты, копирование, кража, иное нарушение злоумышленником режима тайны на защищаемом объекте. Косвенные каналы утечки - потеря или кража

устройств-носителей информации, неправильная утилизация данных, подлежащих уничтожению; дистанционное прослушивание; удаленное управление смарт-устройствами и иное использование интернет-вещей как способа несанкционированного доступа к объекту; радиоперехват сообщений; методы социальной инженерии (соцсети и проч.).

Выполнение задач по защите информационной инфраструктуры экономических субъектов и информации граждан подразумевает проведение мероприятий по физической и технической защите информации на предприятиях, в организациях, информационных системах операторов данных. Безопасность достигается путем ограничения доступа к секретным данным, сохранения их достоверности и целостности в процессе работы с уязвимой информацией. Для защиты информационной инфраструктуры компании или организации применяется комплекс правовых, организационных, программно-аппаратных, инженерно-технических и криптографических мероприятий.

Среди программно-технических средств защиты от утечки конфиденциальной информации – штатные средства защиты информационных системы, а также межсетевые экраны, фильтрующие трафик при передаче его из внутренней сети предприятия во внешний сетевой контур; системы контроля и предупреждения утечки информации (DLP, Data Loss Prevention), позволяющие узнать, кто работал с защищаемой информацией и куда ее передал); IDS-системы (Intrusion Detection System) позволяют обнаружить несанкционированный доступ и попытки атаки на защищаемый ресурс); активные средства защиты, такие как IPS-системы (Intrusion Prevention System) способны ответить на вторжение разрывом соединения или блокировкой трафика злоумышленника и т.п.

Большое значение для предупреждения утечек информации имеют защитные организационные мероприятия, для ограничения доступа и поддержание дисциплины персонала при работе с конфиденциальными сведениями. К организационным мерам защиты можно также отнести сертификацию и аттестацию компонентов информационных систем (с целью установления соответствия защитных мер требованиям безопасности); лицензирование деятельности, связанной с информацией и ее защитой; категорирование информационных объектов по степени конфиденциальности информации и важности защищаемого объекта для социально-экономической инфраструктуры. К организационным мерам защиты информации относятся введение режима конфиденциальности/секретности, в т.ч. издание нормативных и руководящих документов, регламентирующих деятельность персонала, определения перечня защищаемых активов, создание службы безопасности и назначение ответственных за различные аспекты работы с защищаемыми ресурсами, обеспечение служб безопасности необходимыми программно-техническими средствами защиты с учетом продуманной политики информационной безопасности; введение разрешительной системы допуска сотрудников к материалам разной степени секретности, проверка обращения с информацией ограниченного доступа, продуманная методика отбора персонала для работы с секретами, инструктажи и мониторинг использования и защиты секретной информации.

Инженерно-технические мероприятия по защите направлены на создание эффективной системы защиты информационной инфраструктуры (компьютеров, сетей, носителей информации); мероприятия, средства защиты, защищаемые помещения должны отвечать актуальным требованиям нормативных документов РФ и, при необходимости, иметь сертификат соответствия требованиям безопасности, с учетом категорий защищаемой информации. К инженерно-техническим мерам безопасности относятся средства ограничения физического доступа (ограждения, двери, сейфы и т.п., СКУД, средства идентификации персонала; система сигнализации и оповещения о проникновении на объект посторонних лиц и попытке завладения секретной информацией; при необходимости и финансовых возможностях может применяться аппаратура для обнаружения подслушивающих устройств, скрытых видеокамер и других разведывательных приспособлений; приспособления, препятствующие выносу и выводу конфиденциальной информации за пределы защищаемой зоны; средства шифрования обеспечивают защиту конфиденциальной оцифрованную информации при ее хранении и передаче по открытым каналам связи. К криптографическим мерам защиты от искажения информации относятся сертификаты электронной подписи электронных документов; стеганографический метод защиты передаваемой информации путем сокрытия ее в сетевых пакетах и других файлах позволяет сделать передаваемое сообщение невидимым для злоумышленников.

В основе программно-технических систем защиты, применяемых для защиты от утечек секретных сведений экономических субъектов и органов власти, все чаще используются те или иные интеллектуальные технологии (нейросетевые модели, модели знаний, искусственные иммунные системы и генетические алгоритмы и т.д.), облегчающие и ускоряющие решение задач безопасности. В целях повышения безопасности интеллектуальных технологий и обеспечения правовой среды в 2020 г. утверждена программа по созданию в РФ стандартов технологии искусственного интеллекта на 2021–2024 гг., включая стандарты безопасности применения ИИ в транспорте, медицине, образовании, строительстве, стандарта «Умное производство» и др.

Перспективным потенциалом в отношении угроз утечки секретов обладают методы поведенческой аналитики, дополненные возможностями методов машинного обучения. Термином «User and Entity Behavior Analytics» обозначаются системы анализа поведения пользователей и сущностей, выполняющие обработку

данных о поведении пользователей и программных процессов, полученных из различных систем, для обнаружения «поведенческих» аномалий пользователей, процессов, файлов, указывающих на риск несанкционированного доступа и иных воздействий на защищаемые ресурсы. Поведенческий анализ в области информационной безопасности применяется для классификации событий безопасности, для обнаружения и оперативного расследования инцидентов безопасности, для предсказания угроз, для формирования шаблонов «типовой» активности пользователей и программных сущностей для обнаружения аномалий (отклонений в поведении от типовой активности) при их работе с защищаемыми массивами данных. Средствами защиты с технологией UEBA могут выполнять анализ корпоративной почты персонала, сетевой активности работников в локальной сети, обнаруживая нарушение регламентов и ограничений со стороны инсайдеров, «симптомы» утечки данных, а также атаки на защищаемый ресурс; благодаря пополняемой базе профилей поведения персонала и графу коммуникаций с другими субъектами информационной среды, некоторые UEBA-системы могут выполнять прогнозирование поведения пользователей, в т.ч. поведения, угрожающего безопасности защищаемой системы. Подобные системы защиты, в т.ч. построенные с привлечением моделей нейросетей, могут пресекать попытки НСД к защищаемой информации. Однако, как показывает опыт и экспертные суждения, применение нейросетевых моделей для подобных задач не исключает ошибок первого рода (когда система не обнаруживает угрозы в действиях нарушителя) и второго рода (система защиты трактует действия пользователя, осуществляющего легальные операции в информационной системе, попыткой несанкционированного доступа, и либо необоснованно прерывает рабочий процесс, либо сигнализирует о подозрительной активности администратору безопасности). Критичными для нормальной работы могут оказаться подобные ошибки систем безопасности в тех случаях, когда система мешает нормальному функционированию персонала и систем, либо когда она создает «вторичную» уязвимость, будучи призвана закрывать уязвимость для утечек информации. От специалистов безопасности требуется систематически анализировать не только исходные и остаточные уязвимости (после внедрения систем защиты информации), но и неочевидные уязвимости, создаваемые подобными интеллектуальными средствами безопасности в силу несовершенства методологии интеллектуальной автоматизации [3], что является отдельной задачей, решение которой пока не имеет отдельной методики решения в документах отечественных регуляторов, и неочевидно для администраторов безопасности. Дополнительным источником сложности применения средств на основе нейросетей и подобных моделей машинного обучения типа «черный ящик» является то обстоятельство, что нейросетевые системы обнаружения угроз точки принимают решение, не обосновывая решение логически и предлагая администратору безопасности полагаться на веру инструменту защиты или анализировать сигнал о риске угрозы в ручном режиме, что нереально для систем, где атаки исчисляются сотнями в сутки, а требования к скорости реагирования СБИ на угрозы высоки. Применение же моделей интерпретируемого (или «объяснимого» [5], [6]) машинного обучения («interpretable machine learning») в системах информационной безопасности пока не практикуется, насколько нам известно.

Повышение информационной безопасности требует проведения комплексных мероприятий с использованием сложных технических устройств. Необходимостью становится возможность правильно оценивать степень риска утечки информации, а также «вторичные» риски, создаваемые интеллектуальными автоматизированными системами защиты от угроз ИБ. Важно постоянно анализировать эффективность информационной защиты и совершенствовать методику ее проведения.

Список литературы:

1. Федеральный проект «Искусственный интеллект» – URL: <https://digital.ac.gov.ru/about/5055> (дата обращения: 26.11.2021)
2. Министерства подготовят дорожные карты по внедрению решений на основе искусственного интеллекта / Сайт Правительства России. 2020. 24 августа. URL: <https://ac.gov.ru/news/page/ministerstva-podgotovat-doroznye-karty-po-vnedreniuresenij-na-osnove-iskusstvennogo-intellekta-26685> (дата обращения: 25.11.2021)
3. Миронова Н.Г. Философское осмысление социальных рисков интеллектуальной автоматизации социального управления // Цифровой ученый: лаборатория философа. 2021. Т. 4. № 2. С. 125-144. DOI: 10.32326/2618-9267-2021-4-2-125-144 . <https://www.elibrary.ru/item.asp?id=47145602> (дата обращения 26.11.2021)
4. Вострецова В. Е. Основы информационной безопасности: научная литература / В. Е. Вострецова — Издательство Уральского университета, 2019. — С. 92.
5. Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., Herrera, F. “Explainable Artificial Intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI”, Information Fusion, 2020, vol. 58, pp. 82–115. Available at: <https://www.sciencedirect.com/science/article/pii/S1566253519308103> (accessed on June 1, 2021).
6. Knight, 2017, web – Knight W. DARPA is funding projects that will try to open up AI’s black boxes // MIT Technology Review. April 13, 2017. URL: <https://www.technologyreview.com/2017/04/13/152590/the-financial-worldwants-to-open-ais-black-boxes> (дата обращения: 20.04.2021).

References

1. Federal project «Artificial Intelligence» - URL: <https://digital.ac.gov.ru/about/5055> (date of access: 11/26/2021) (In Russian)
2. The ministries will prepare roadmaps for the implementation of solutions based on artificial intelligence / Russian Government website. 2020.24 August. URL: <https://ac.gov.ru/news/page/ministerstva-podgotovat-doroznye-karty-po-vnedreniuresenij-na-osnove-iskusstvennogo-intellekta-26685> (date of access: 25.11.2021) (In Russian)
3. Mironova N.G. Philosophical understanding of social risks of intellectual automation of social management // TSifrovoy uchenyi laboratoriii filsofa. 2021. T. 4. No. 2. S. 125-144. DOI: 10.32326 / 2618-9267-2021-4-2-125-144 <https://www.elibrary.ru/item.asp?id=47145602> (date of access 11/26/2021) (In Russian)
4. Vostretsova V.E. Fundamentals of information security: scientific literature / E.V. Vostretsova - Publishing house of the Ural University, 2019. - P. 92. (In Russian)
5. Arrieta, A.B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., Herrera, F. “Explainable Artificial Intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI”, Information Fusion, 2020, vol. 58, pp. 82–115. Available at: <https://www.sciencedirect.com/science/article/pii/S1566253519308103> (accessed on June 1, 2021).
6. Knight, 2017, web – Knight W. DARPA is funding projects that will try to open up AI’s black boxes // MIT Technology Review. April 13, 2017. URL: <https://www.technologyreview.com/2017/04/13/152590/the-financial-worldwants-to-open-ais-black-boxes> (дата обращения: 20.04.2021).