Московский экономический журнал. № 5. 2023
Moscow economic journal. № 5. 2023
Научная статья
Original article
УДК 338.242.2
doi: 10.55186/2413046X_2023_8_5_238

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ В ПРОЦЕССЕ ТРАНСФЕРА ТЕХНОЛОГИЙ

INFORMATION SECURITY OF OBJECTS OF EXCLUSIVE RIGHTS IN TECHNOLOGY TRANSFER

Сердечный Денис Владимирович, к.т.н., доцент кафедры управления инновациями, ФГБОУ ВО Государственный университет управления, E-mail: dv_serdechnyj@guu.ru

Serdechnyy Denis Vladimirovich, PhD, Associate Professor of the Department of Innovation Management, State University of Management, E-mail: dv_serdechnyj@guu.ru

Аннотация. В статье приведены результаты исследований инструментов обеспечения информационной безопасности результатов интеллектуальной деятельности – объектов исключительных прав в процессе передачи технологий. Объекты, обладающие исключительными правами и знаниями, нуждаются в особом внимании к их информационной безопасности в процессе трансфера технологий. Подчеркиваются важность наличия эффективных мер информационной безопасности при передаче конфиденциальной информации и технологий, связанных с исключительными правами. Современные технологии позволяют значительно ускорить и упростить процесс трансфера, однако это может привести к утечкам информации и нарушениям права на интеллектуальную

собственность. Особенности обеспечения информационной безопасности объектов с исключительными правами включают не только технические меры, но и организационные и правовые аспекты. Необходимость обеспечения информационной безопасности объектов с исключительными правами должна учитываться на всех этапах процесса - от разработки технологий до заключения договоров. Основными мерами обеспечения информационной безопасности при трансфере технологий являются аутентификация пользователей, шифрование данных, контроль доступа, мониторинг и аудит безопасности. Важно учитывать национальные и международные законы и стандарты, которые могут ограничить доступ к технологиям или требовать специального разрешения на их трансфер. Обмен технологиями и знаниями должен осуществляться только с добросовестными, надежными контрагентами, которые также обеспечивают высокий уровень информационной безопасности и не злоупотребляют полученными знаниями. Эффективное обеспечение информационной безопасности технологического трансфера позволяет, в том числа. повышает уровень конкурентоспособности В статье также анализируются проблемы, возникающие при передаче технологий, и приводятся рекомендации по улучшению безопасности передачи данных и объектов исключительных прав. обладателей объектов исключительных прав.

Abstract. The article presents the results of studies of tools for ensuring information security of the results of intellectual activity - objects of exclusive rights in the process of technology transfer. Objects with exclusive rights and knowledge need special attention to their information security in the process of technology transfer. The importance of having effective information security measures in the transfer of confidential information and technologies associated with exclusive rights is emphasized. Modern technologies can significantly speed up and simplify the transfer process, but this can lead to information leaks and violations of intellectual property rights. Features of ensuring the information security of objects with exclusive rights include not only technical measures, but

also organizational and legal aspects. The need to ensure the information security of objects with exclusive rights should be taken into account at all stages of the process - from the development of technologies to the conclusion of contracts. The main measures to ensure information security in technology transfer are user authentication, data encryption, access control, security monitoring and auditing. It is important to consider national and international laws and standards that may restrict access to technology or require special permission to transfer it. The exchange of technologies and knowledge should be carried out only with conscientious, reliable counterparties who also ensure a high level of information security and do not abuse the acquired knowledge. Effective provision of information security of technology transfer allows, among other things. improves competitiveness The article also analyzes the problems that arise in the transfer of technologies, and provides recommendations for improving the security of data transfer and objects of exclusive rights. owners of objects of exclusive rights.
Ключевые слова: информационная безопасность, субъект цифровой экономики, трансфер технологий, секреты производства, исключительные права, инновационное предприятие
Keywords: cybersecurity, subject of the digital economy, technology transfer, production secrets, exclusive rights, innovative enterprise

Информационная безопасность имеет критическое значение для процессов трансфера технологий, поскольку такие процессы зачастую включают передачу конфиденциальной информации, секретов производства и других объектов исключительных прав между субъектами цифровой экономики – инновационными предприятиями. Несоблюдение мер информационной безопасности может привести к утечке важной информации, что может повредить бизнес-планам, репутационным рискам и т.п.

Кроме того, компании могут столкнуться с кибератаками и кражей данных, если не уделяют достаточного внимания информационной

безопасности при проведении процессов передачи технологий. Необходимо соблюдать строгие меры безопасности, включая защиту данных, криптографию, аутентификацию и контроль доступа. Это позволит защитить конфиденциальную информацию и гарантировать, что процессы трансфера технологий будут проводиться безопасно и эффективно [1].

Объекты исключительных прав, которые могут быть переданы от одного субъекта цифровой экономики другому в процессе трансфера технологий: патенты; авторские права; товарные знаки; секреты производства (ноу-хау); описание производственных процессов; техническая документация (включая технические рисунки, спецификации, инструкции по эксплуатации); информационные базы данных и программное обеспечение, используемое для трансфера технологий; лицензионные соглашения и контракты, включая права на производство, использование и распространение технологий; техническая помощь и консультационные услуги, включая обучение и сопровождение внедрения технологии на практике [2].

Утечки конфиденциальной информации. технологии и знания, передаваемые от одного предприятия к другому, могут содержать конфиденциальную информацию, которая, если попадет в руки конкурентов, может привести к серьезным последствиям для бизнеса и экономики в целом.

Передача технологий может привести к нарушению авторских прав и интеллектуальной собственности, если получающая сторона не будет соблюдать права и условия передачи знаний. К тому же, правоприобретатель может использовать полученные технологии не только для улучшения своей позиции на рынке, но и для вредоносных действий. Если передаваемые технологии включают в себя информацию о средствах защиты информации, то недостатки в этих средствах могут стать лазейкой для киберпреступников.

Ошибки в организации процесса трансфера технологий могут привести к различным проблемам, включая задержки, утечки информации, качественные и квалификационные проблемы: нарушения доступа к данным; низкую безопасность паролей и авторизационных данных; нежелательная

почта и спам, включая поддельные сообщения и мошенничества; кража устройств хранения данных; атаки вирусов, червей и троянов; несанкционированный доступ к сети и попытки идентификации сетей [3].

К инструментам обеспечения информационной безопасности процессов трансфера технологий можно отнести антивирусные программы и брандмауэры; системы управления доступом; криптографические средства защиты информации; методы интеллектуального анализа данных [4,5].

Технологии трансфера могут быть уязвимыми для различных видов атак и угроз информационной безопасности. Для обеспечения безопасности процессов трансфера технологий необходимо использовать специальные инструменты, такие как системы шифрования и авторизации доступа.

Контроль доступа к конфиденциальной информации, включая научные исследования и разработки, является важным аспектом обеспечения безопасности в процессе трансфера технологий. Важную роль в процессе обеспечения информационной безопасности процессов трансфера технологий играют требования к защите данных, которые должны быть регулированы определенными стандартами и правилами. Разработка и реализация эффективных инструментов информационной безопасности является ключевым фактором для увеличения уровня защиты в процессе трансфера технологий и предотвращения утечек и краж конфиденциальной информации [6].

Комплексный подход к обеспечению информационной безопасности процессов трансфера технологий предполагает использование различных мероприятий и технологий для защиты информации на всех этапах передачи технологии от исходной организации-разработчика до принимающей организации. Ниже приведены основные элементы комплексного подхода к обеспечению информационной безопасности процессов трансфера технологий:

1. Анализ системы безопасности и инфраструктуры. Необходимо оценить уровень защищенности информационной системы и

инфраструктуры организации, осуществляющей трансфер технологий. При этом учитываются как физические, так и логические меры безопасности.

2. Анализ рисков. Необходимо провести предварительный анализ рисков, связанных с трансфером технологий, чтобы определить потенциальные опасности для конфиденциальности, целостности и доступности информации.

3. Разработка стратегии безопасности. Разработка стратегии безопасности проводится на основе анализа системы безопасности и инфраструктуры, анализа рисков и определения требований к безопасности. Стратегия безопасности определяет меры по защите информации во время трансфера технологий.

4. Использование шифрования. При передаче конфиденциальной информации рекомендуется использовать шифрование для защиты от несанкционированного доступа.

5. Использование вопросно-ответных систем. Для защиты от вредоносных программ и хакерских атак можно использовать вопросно-ответные системы, которые позволяют проверять подлинность пользователя перед предоставлением доступа к системе.

6. Обучение сотрудников. Сотрудникам, участвующим в процессе трансфера технологий, необходимо предоставить обучение и инструкции по безопасности, чтобы они понимали, как действовать в случае возникновения угрозы информационной безопасности.

7. Применение многофакторной аутентификации. Для повышения уровня безопасности можно использовать многофакторную аутентификацию, которая включает в себя не только пароль, но и другие факторы, такие как отпечатки пальцев или биометрические данные.

8. Регулярное тестирование системы безопасности. Один из важных элементов обеспечения информационной безопасности - это проведение регулярных тестов на проникновение, которые позволяют определить слабые места в системе и своевременно принять меры по устранению уязвимостей.

Комплексный подход к обеспечению информационной безопасности процессов трансфера технологий позволяет минимизировать риски и обеспечить безопасный и надежный процесс передачи технологий [7].

Оценка эффективности инструментов обеспечения информационной безопасности должна проводиться с учетом нескольких факторов. Инструменты должны соответствовать стандартам и рекомендациям по информационной безопасности. Они должны обеспечивать защиту от угроз, а также предотвращать возможные уязвимости. Эффективность инструментов может быть определена по скорости их работы, возможности обеспечения быстрого реагирования на угрозы и выявление в том числе скрытых угроз.

Инструменты должны иметь возможность масштабироваться в зависимости от объема и специфики защищаемой информации. Инструменты должны быть просты в использовании даже для неопытных пользователей. Необходимо учитывать, насколько продукт интуитивно понятен и прост в установке и настройке.

Оценка эффективности инструментов обеспечения информационной безопасности может проводиться с помощью пилотного проекта, когда конкретная система защиты внедряется на определенное время на определенном участке информационной инфраструктуры. В ходе пилотного проекта можно оценить эффективность системы и провести корректировку в случае необходимости. Оценка эффективности должна учитывать затраты на приобретение, установку и обновление инструмента. Инструмент должен быть совместим с существующей инфраструктурой предприятия, чтобы уменьшить затраты на обновление системы. К тому же эффективность инструмента полностью зависит от его надежности и стабильности в работе. Инструмент должен позволять детектировать угрозы быстро и эффективно, а также давать возможность последующей реакции на них [8-11].

Система безопасности является важным компонентом любой организации, включая компании, правительства и учреждения. Данная система включает в себя политики, процедуры, технологии и людей, которые

заботятся о защите данных и информации организации. Однако, современные угрозы постоянно меняются, поэтому необходимо постоянное обновление и улучшение системы безопасности.

В первую очередь, необходимо оценивать риски и уязвимости системы на регулярной основе, чтобы выявлять новые угрозы и разрабатывать меры для их предотвращения. Далее, следует обновлять программное и аппаратное обеспечение, чтобы гарантировать безопасность системы от новых угроз и противостоять множественным методам хакеров и вредоносных программ.

Также необходимо обеспечить обучение и повышение квалификации персонала по вопросам безопасности. Сотрудники должны знать, какие наиболее распространенные виды атак и угрозы, а также осознавать свою важность в защите данных и информации организации.

Наконец, система безопасности должна постоянно развиваться и улучшаться для более эффективной защиты от новых и изменяющихся угроз. Кроме того, она должна быть подвержена регулярным проверкам и аудитам для поиска недостатков и выявления возможных уязвимостей.

В целом, поддержание безопасности системы является постоянным процессом, который требует регулярного обновления и улучшения. Реализация этих мер позволит организациям обеспечить безопасность своих данных и информации.

Список источников

1. Зегжда Д.П., Васильев Ю.С., Полтавцева М. А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. №2 (26).

2. Близнец И.А. Интеллектуальная собственность в современном мире: монография. – М.: Проспект, 2017. – 669с.

3. Меры защиты конфиденциальной информации: правовые, организационные, технические и способы их реализации [Электронный

ресурс] // URL: https://rt-solar.ru/products/solar_dozor/blog/2084/ (дата обращения : 19.04.2023). – Текст : электронный.

4. Poddar S., Banerjee S., Ghosh M. Technology Transfer in Spatial Competition when Licensees are Asymmetric // The Manchester School. – 2021. Vol. 89, Is. 1. – pp. 24–45.

5. Безопасность современных информационных технологий : монография / Е. В. Стельмашонок [и др.]; под общ. ред. Е. В. Стельмашонок. – СПб. : СПбГИЭУ, 2012. – 408 с.

6. Poticha D., Duncan M. Intellectual Property – The Foundation of Innovation: A Scientist's Guide to Intellectual Property // Journal of Mass Spectrometry. – 2019. Vol. 54, Is. 3. – pp. 288–300.

7. Zaydi, Mounia & Bouchaib, Nassereddine. (2018). Toward a New Integrated Approach of Information Security Based on Governance, Risk and Compliance. 10.1007/978-3-030-03577-8_37.

8. Ажмухамедов И.М., Ханжина Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности // ВестникАстраханского государственного технического университета. Серия: Экономика. — 2011. — № 1. — С. 185–190.

9. Uchida H. The Big Push to a Knowledge-based Economy with Intellectual Property Rights Protection // Review of Development Economics. – 2020. Vol. 24, Is. 4. – pp. 1551–1559.

10. Aubuchon K. Applying NPV and ROI to Security Investment Decisions. — Washington, DC: U.S. — 2015. — P. 65–74.

11. Антонова Е.К., Баранова Е.К., Бабаш А.В. Особенности оценки экономической эффективности системы защиты информации // Материалы 26-й научно-практической конференции «Методы и технические средства обеспечения безопасности информации», 26–29 июня 2017. — СПб.: Изд-во Политехнического университета — 2017. — С. 68–77.

References

1. Zegzhda D.P., Vasiliev Yu.S., Poltavtseva M.A., Kefeli I.F., Borovkov A.I. Cybersecurity of progressive production technologies in the era of digital transformation // Issues of cybersecurity. 2018. No. 2 (26).

2. Twin I.A. Intellectual property in the modern world: monograph. – M.: Prospekt, 2017. – 669s.

3. Measures to protect confidential information: legal, organizational, technical and methods of their implementation [Electronic resource] // URL: https://rt-solar.ru/products/solar_dozor/blog/2084/ (date of access: 19.04.2023) . – Text : electronic.

4. Poddar S., Banerjee S., Ghosh M. Technology Transfer in Spatial Competition when Licensees are Asymmetric // The Manchester School. – 2021. Vol. 89, Is. 1.-pp. 24–45.

5. Security of modern information technologies: monograph / E. V. Stelmashonok [and others]; under total ed. E. V. Stelmashonok. - St. Petersburg. : SPbGIEU, 2012. - 408 p.

6. Poticha D., Duncan M. Intellectual Property – The Foundation of Innovation: A Scientist’s Guide to Intellectual Property // Journal of Mass Spectrometry. – 2019. Vol. 54, Is. 3.-pp. 288–300.

7. Zaydi, Mounia & Bouchaib, Nassereddine. (2018). Toward a New Integrated Approach of Information Security Based on Governance, Risk and Compliance. 10.1007/978-3-030-03577-8_37.

8. Azhmukhamedov I.M., Khanzhina T.B. Evaluation of the economic efficiency of measures to ensure information security // Bulletin of the Astrakhan State Technical University. Series: Economy. - 2011. - No. 1. - S. 185–190.

9. Uchida H. The Big Push to a Knowledge-based Economy with Intellectual Property Rights Protection // Review of Development Economics. – 2020. Vol. 24, Is. 4.-pp. 1551–1559

10. Aubuchon K. Applying NPV and ROI to Security Investment Decisions. — Washington, DC: U.S. — 2015. — P. 65–74.

11. Antonova E.K., Baranova E.K., Babash A.V. Features of assessing the economic efficiency of the information security system // Proceedings of the 26th scientific and practical conference "Methods and technical means of ensuring information security", June 26-29, 2017. - St. Petersburg: Publishing House of the Polytechnic University - 2017. - P. 68- 77.

Для цитирования: Сердечный Д.В. Особенности обеспечения информационной безопасности объектов исключительных прав в процессе трансфера технологий // Московский экономический журнал. 2023. № 5. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-5-2023-40/