УДК 004.056.5

Н.Р. Коковин[1], Н.И. Глухов[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ ДАННЫХ ПРИ УВОЛЬНЕНИИ СОТРУДНИКОВ В КОММЕРЧЕСКИХ СТРУКТУРАХ

Аннотация. *Настоящая статья рассматривает актуальную проблему в современных организациях, где конфиденциальная информация является важным активом компаний, однако в силу разных причин режим коммерческой тайны в них не установлен. Авторы отмечают, что увольнение сотрудников представляет потенциальный риск утечки ценных данных.*

В данной статье обсуждается влияние политики информационной безопасности на процесс увольнения сотрудников, подчеркивается необходимость строгого соблюдения правил и процедур, направленных на минимизацию рисков утечки данных и сохранение информации. В тексте приведены основные аспекты политики информационной безопасности, рекомендованные к внедрению в коммерческих структурах.

Ключевые слова: *увольнение сотрудников, политика информационной безопасности, информационная безопасность, конфиденциальная информация, режим коммерческой тайны.*

N.R. Kokovin[1], N.I. Glukhov[1]

[1]Irkutsk State Transport University, Irkutsk, the Russian Federation

SOME ASPECTS OF DATA PROTECTION DURING EMPLOYEE OFFBOARDING IN COMMERCIAL ORGANIZATIONS

Abstract. *This article addresses a pressing issue in modern organizations, where confidential information is a critical asset, yet trade secret policies are often not formally established for various reasons. The authors highlight that employee offboarding poses a potential risk of sensitive data leakage.*

The study examines the impact of information security policies on the employee termination process, emphasizing the need for strict adherence to rules and procedures aimed at minimizing data breach risks and safeguarding information. The paper outlines key aspects of information security policies recommended for implementation in commercial enterprises.

Key words: *employee termination, information security policy, data protection, confidential information, trade secret regime.*

Введение

С каждым днём важность обеспечения информационной безопасности становится все более актуальной для организаций по всему миру, особенно в Российской Федерации. Согласно статистике, каждый пятый сотрудник в российской ИТ-компании плохо знает основы информационной безопасности [1]. Около половины сотрудников обладают средними знаниям в данной области, остальные – хорошими. Следует отметить, что статистика приведена среди компаний в сфере информационных технологий, которые лучше остальных организаций понимают важность обеспечения информационной безопасности. Уровень подготовки персонала в компаниях, основная деятельность которых не связана напрямую с информационными технологиями, следует считать ещё ниже.

Несмотря на это в большинстве организаций информационная безопасность в той или иной степени присутствует. Минимальный уровень защиты информации чаще всего представляет собой соглашение субъекта персональных данных (сотрудника) на обработку таких данных, установление парольной политики на автоматизированных рабочих местах, а также наличие физической защиты в виде сейфов и охранной сигнализации. Также, особо важным аспектом в обеспечении защиты информационных активов предприятий является такой локальный документ, как политика информационной безопасности. Однако, анализируя существующие политики в организациях, можно отметить, что недостаточно внимания

уделяется вопросам, посвященным увольнению сотрудников, особенно работающих с конфиденциальной информацией.

В данной связи особо уязвимы коммерческие структуры, в которых по тем или иным причинам не установлен режим коммерческой тайны. Ввиду отсутствия данного режима необходима проработка вопроса обеспечения защиты конфиденциальной информации при увольнении сотрудников. Учитывая, что процесс увольнения представляет собой потенциальный источник угрозы для конфиденциальности и целостности ценной информации, эффективное управление этим процессом неотъемлемо для поддержания информационной безопасности в коммерческих структурах.

Режим коммерческой тайны

Организации, в которых установлен режим коммерческой тайны, лучше остальных способны предотвратить инциденты информационной безопасности. Это связано с тем, что защита коммерческой тайны регламентирована законодательно [2]. Установление данного режима подразумевает от обладателя информации наличия перечня информации, составляющей коммерческую тайну; ограничения доступа к такой информации с соответствующим контролем установленного порядка обращения с ней; учёта лиц, получивших доступ к конфиденциальным сведениям, а также тех, кому они были предоставлены или переданы; нанесения на материальные носители информации грифа «Коммерческая тайна», а также регулирование отношений по использованию работниками и контрагентами сведений, составляющих коммерческую тайну. Последнее, в том числе, подразумевает подписание соглашения о неразглашении информации, составляющей коммерческую тайну. Более того, Федеральный закон № 98-ФЗ обязывает работников не разглашать информацию, составляющую коммерческую тайну, в течение всего срока действия данного режима, в том числе после прекращения действия трудового договора.

Если же в коммерческой структуре не установлен режим коммерческой тайны, то в случае её разглашения организация, являющаяся обладателем конфиденциальных сведений, не сможет ссылаться на Федеральный закон «О коммерческой тайне» для возмещения убытков, связанных с нарушением конфиденциальности, целостности или доступности таких сведений. Таким образом, единственным способом обеспечить защиту ценной информации является организация соответствующей корпоративной культуры, а именно: создание и внедрение политики информационной безопасности. Особенно остро данный вопрос стоит в рамках увольнения работников в связи с тем, что бывший сотрудник может использовать информацию, полученную в процессе рабочей деятельности, для своей выгоды (или конкурентного преимущества нового работодателя) в ущерб обладателю информации.

Роль и содержание политики информационной безопасности в контексте увольнения

В основе успешной защиты конфиденциальной информации при увольнении персонала лежит разработка и строгое соблюдение политики информационной безопасности организации. Политика информационной безопасности представляет собой совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [3]. В контексте увольнения сотрудников политика информационной безопасности определяет стратегию и меры, необходимые для минимизации рисков утечки информации и недобросовестного использования данных.

Ниже представлены ключевые аспекты защиты данных при увольнении сотрудников, которые следует учесть в политике информационной безопасности:

1. Процедуры управления доступом.

Политика должна определять процедуры управления доступом к информационным ресурсам и системам организации в случае увольнения сотрудника. Данный раздел включает в себя оперативное ограничение доступа к конфиденциальным данным и системам, а также административные процедуры по снятию прав доступа с увольняемого сотрудника.

2. Проведение аудита доступа.

В политике должно быть предусмотрено проведение аудита доступа к информационным ресурсам перед увольнением сотрудника. Эта процедура позволит выявить и устранить любые несанкционированные или ненужные права доступа, которые могли сохраниться у сотрудника в течение его работы в организации.

3. Процедуры удаления данных.

Также, в политике необходимо изложить процедуры и инструкции по удалению или архивированию данных, которые принадлежат увольняемому сотруднику. Сюда относится удаление конфиденциальной информации с персональных устройств сотрудника, а также удаление его аккаунтов и прав доступа к корпоративным ресурсам. В случае, если сотруднику выдавались какие-либо технические средства для исполнения своих должностных обязанностей, например, флеш-накопитель информации, ноутбук, телефон, то необходимо также регламентировать ведение соответствующих журналов учёта техники.

4. Обучение сотрудников.

Как показывает практика, документы, связанные с информационной безопасностью, сотрудник организации видит первый и последний раз при устройстве на работу. Будущий работник подписывает лист ознакомления с данными документами совместно с трудовым договором, прочитав их без особой внимательности в отделе кадров. Отсутствие должного обучения информационной безопасности, напоминания правил и политик, инструктирования и сопровождения в течение рабочей деятельности сотрудников со стороны соответствующих специалистов приводит к тому, что 30% сотрудников используют одинаковый пароль для нескольких учётных записей, а около 40% – одни и те же учётные данные для входа как в личные, так и в рабочие сервисы [4].

В политике следует предусмотреть условия обучения сотрудников и руководителей по процедурам увольнения и безопасности информации. Данные мероприятия позволяют повысить осведомлённость персонала о важности обеспечения безопасности данных во время и после увольнения и снижают риск возможных инцидентов информационной безопасности.

5. Ответственность за нарушение.

Отдельно следует выделить ответственность за нарушение политики информационной безопасности. В соответствии с действующим законодательством Российской Федерации к нарушителю могут применяться следующие меры наказания: дисциплинарная ответственность (замечание, выговор, увольнение) [5], административная ответственность (штраф) [6], гражданско-правовая ответственность (возмещение убытков) [7], уголовная ответственность (штраф, либо ограничение/лишение свободы) [8].

Разработка и внедрение политики информационной безопасности

Важно отметить, что разработка политики информационной безопасности должна проводиться в тесном непосредственном сотрудничестве с руководством организации. Данный документ будет эффективен только в том случае, когда он не противоречит видению и стратегии руководства. То есть, руководящий состав организации должен быть заинтересован в соблюдении сотрудниками правил политики информационной безопасности, а также самостоятельно придерживаться их.

Также, политику информационной безопасности следует внедрить в общую корпоративную культуру и процессы управления организацией. Поддержке политики поспособствует создание таких необходимых инструментов и ресурсов, как шаблоны организационно-распорядительной документации, должностные инструкции, согласия о неразглашении. Важно отметить, что шаблонные документы нуждаются в адаптации под специфику и структуру организации, ведь в противном случае они будут лишь формальностью, а их эффективность станет крайне низкой.

Регулярное оценивание эффективности, внесение корректировок и обновление политики информационной безопасности позволит своевременно устранять уязвимости и соблюдать требования законодательства в случае каких-либо внешних и внутренних изменений.

Психологический аспект увольнения

Дополнительно следует акцентировать внимание на психологическом аспекте увольнения сотрудников. Сам факт увольнения является стрессовой ситуацией, причём зачастую не только для работника, но и для работодателя. С точки зрения информационной безопасности особый интерес представляет вопрос, касающийся эмоционального фона процесса увольнения, ведь если он негативный, то бывший работник может стать потенциальным нарушителем. Так, в российских компаниях уволенные сотрудники часто считают себя несправедливо обиженными и на волне эмоций начинают мстить. Исследования, проводившиеся в данной области, показали, что довольно распространенный способ мести – намеренное удаление из рабочего компьютера информации, которая представляет ценность для работодателя [9]. Также, бывший сотрудник может использовать наработанную клиентскую базу в своих интересах, например, для получения преимущества при дальнейшем трудоустройстве.

С целью предотвращения подобных ситуаций и минимизации рисков нанесения ущерба информационным активам предприятия, следует проводить проблемно-центрированную беседу в период, предстоящий увольнению сотрудника, а также комплекс мероприятий для смягчения процедуры увольнения [10]. Ещё одним действенным способом будет составление рекомендательного письма или характеристики работника для дальнейшего предоставления потенциальным работодателям. Беседа касательно прав и возможностей по использованию конфиденциальных сведений, полученных в процессе рабочей деятельности, настоятельно рекомендуется авторами данной статьи, особенно для коммерческих структур, в которых не установлен режим коммерческой тайны.

Заключение

Данная статья подчёркивает важность разработки и соблюдения политики информационной безопасности организации при увольнении сотрудников. Реализация эффективной политики не только защищает конфиденциальные данные, но и снижает риски нанесения ущерба информационной безопасности коммерческим структурам, особенно в которых не установлен режим коммерческой тайны. Разработка стратегий управления доступом, аудита доступа, процедур удаления данных, обучения персонала и определение ответственности за нарушения являются ключевыми шагами для обеспечения безопасного увольнения сотрудников. Постоянное обновление и оценка эффективности политики обеспечивают адаптацию к изменяющимся условиям и требованиям безопасности данных, а психологические беседы с сотрудниками минимизируют риски использования конфиденциальных сведений с целью причинения умышленного вреда бывшему работодателю.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационная безопасность в компании // Tadviser [Электронный ресурс] / URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_компании.
2. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) // СПС «КонсультантПлюс».
3. ГОСТ Р 50922-2006. Группа Э00. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.
4. Более 60% офисных работников обходят политику кибербезопасности // Компания «Информзащита» [Электронный ресурс] / URL: https://www.infosec.ru/press-center/news/bolee-60-ofisnykh-rabotnikov-obkhodyat-politiku-kiberbezopasnosti/.
5. Трудовой кодекс Российской Федерации: от 30.12.2001 № 197-ФЗ (ред. от 06.04.2024) // СПС «КонсультантПлюс».
6. Кодекс Российской Федерации об административных правонарушениях: от 30.12.2001 № 195-ФЗ (ред. от 22.04.2024) // СПС «КонсультантПлюс».
7. Гражданский кодекс Российской Федерации (часть четвёртая): от 18.12.2006 № 230-ФЗ (ред. от 14.12.2023) // СПС «КонсультантПлюс».

8. Уголовный кодекс Российской Федерации: от 13.06.1996 № 63-ФЗ (ред. от 06.04.2024) // СПС «КонсультантПлюс».

9. Как работодателям мстят обиженные сотрудники // Сетевое издание Ведомости [Электронный ресурс] / URL: https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki.

10. Алексеева, Е. А. Особенности управления стрессом при увольнении сотрудников / Е. А. Алексеева, О. А. Лозинская // Современное образование: интеграция науки и практики : Сборник публикаций преподавателей и студентов по итогам международных научно-практических конференций в апреле 2024 года, Москва, 15 апреля 2024 года. – Москва: Издательство «Перо», 2024. – С. 5-10.

REFERENCES

1. Information Security in Companies // Tadviser [Electronic resource] / URL: https://www.tadviser.ru/index.php/Article:Information_security_in_companies.

2. Federal Law «On Commercial Secrets» N 98-FZ of July 29, 2004 (as amended on August 8, 2024) // ConsultantPlus Legal Reference System.

3. GOST R 50922-2006. Group E00. National Standard of the Russian Federation. Information Protection. Basic Terms and Definitions.

4. Over 60% of Office Workers Bypass Cybersecurity Policies // Informzashita Company [Electronic resource] / URL: https://www.infosec.ru/press-center/news/bolee-60-ofisnykh-rabotnikov-obkhodyat-politiku-kiberbezopasnosti/.

5. Labor Code of the Russian Federation N 197-FZ of December 30, 2001 (as amended on April 6, 2024) // ConsultantPlus Legal Reference System.

6. Code of Administrative Offenses of the Russian Federation N 195-FZ of December 30, 2001 (as amended on April 22, 2024) // ConsultantPlus Legal Reference System.

7. Civil Code of the Russian Federation (Part Four) No. 230-FZ of December 18, 2006 (as amended on December 14, 2023) // ConsultantPlus Legal Reference System.

8. Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as amended on April 6, 2024) // ConsultantPlus Legal Reference System.

9. How Disgruntled Employees Take Revenge on Employers // Vedomosti Online Edition [Electronic resource] / URL: https://www.vedomosti.ru/management/articles/2016/12/08/668700-rabotodatelyam-mstyat-sotrudniki.

10. Alekseeva, E. A., & Lozinskaya, O. A. (2024). Specifics of Stress Management During Employee Termination. Modern Education: Integration of Science and Practice: Collection of Publications Based on the Results of International Scientific-Practical Conferences in April 2024, Moscow, April 15, 2024 (pp. 5-10). Moscow: Pero Publishing House.

Информация об авторах

Коковин Никита Русланович – студент 2-го курса магистратуры по специальности Информационная безопасность. Безопасность информационных систем и технологий, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: kokovin.nikita01@gmail.com

Глухов Николай Иванович – канд. экон. наук, доцент каф. информационных систем и защиты информации, Иркутский государственный университет путей сообщения, г. Иркутск e-mail: gni1953@mail.ru

Information about the authors

Kokovin Nikita Ruslanovich – 2nd-year Master's student in the specialty Information Security. Security of Information Systems and Technologies, Irkutsk State Transport University (Irkutsk, Russia), email: kokovin.nikita01@gmail.com.

Glukhov Nikolay Ivanovich – Candidate of Economic Sciences, Associate Professor at the Department of Information Systems and Information Protection, Irkutsk State Transport University (Irkutsk, Russia), email: gni1953@mail.ru