DOI 10.37882/2223-2966.2023.07.39

ЭКОНОМИЧЕСКАЯ И КАДРОВАЯ БЕЗОПАСНОСТЬ КОМПАНИИ В ЧАСТИ ПРОТИВОДЕЙСТВИЯ ИНСАЙДЕРСКОЙ УГРОЗЕ

ECONOMIC AND PERSONNEL SECURITY OF THE COMPANY IN TERMS OF COUNTERING THE INSIDER THREAT

V. Strizhkov

Summary: The article discusses insider threats in companies from different sectors and various methods for assessing them. The problem of information leakage is becoming more and more relevant for companies in all areas of economic activity, as a company can incur losses not only due to information leakage about its inventions, but also through lawsuits in case of theft of personal information of customers or contractors. This means that in order to gain access to international markets, Russian companies must have an appropriate level of protection not only for confidential information, but also for data on customers, contractors, etc. The purpose of the article is to analyze the existing methodological approaches to assessing insider threats in an enterprise as a and economic security. Different industries have different vulnerabilities to insider threats and should have appropriate approaches to managing insider threats. The study found that information leaks pose a serious threat to the economic and personnel security of the company. Today, there are significant improvements and the emergence of effective procedures to counter external threats, but protection against insider attacks remains quite low. In the course of the study, the concept of an insider attacker was defined, the types of insider threats were identified, and the main actions of personnel before an insider attack were identified. It has been proven that the degree of insider threat is determined by the nature of the company's activities and the liquidity of information that can become the subject of a leak. Most of the leaks are observed in high-tech companies and medical institutions, while the most liquid is the information of banks, financial institutions, industrial and commercial companies.

Keywords: corporate economic security, human capital, personnel security, insider threat, information database.

Стрижков Владислав Александрович
Аспирант, Финансовый университет при Правительстве Российской Федерации (г. Москва)
218668@edu.fa.ru

Аннотация. В статье рассматриваются инсайдерские угрозы в компаниях из разных секторов и различные методы их оценки. Проблема утечки информации становится все более актуальной для компаний всех сфер экономической деятельности, так как компания может нести убытки не только из-за утечки информации о своих изобретениях, но и через судебные иски в случае кражи личной информации заказчиков или подрядчиков. Это означает, что для получения доступа к международным рынкам российские компании должны иметь надлежащий уровень защиты не только конфиденциальной информации, но и данных о заказчиках, контрагентах и т.д. Целью статьи является анализ существующих методологических подходов к оценке инсайдерских угроз на предприятии как составляющей кадровой и экономической безопасности. Разные отрасли имеют разную уязвимость к инсайдерским угрозам и должны иметь соответствующие подходы к управлению инсайдерскими угрозами. В исследовании установлено, что утечки информации представляют серьезную угрозу экономической и кадровой безопасности компании. Сегодня отмечаются значительные улучшения и появление эффективных процедур противодействия внешним угрозам, однако защита от инсайдерских атак остается достаточно низкой. В ходе исследования было определено понятие инсайдера, установлены виды инсайдерских угроз, а также обозначены основные действия персонала перед инсайдерской атакой. Доказано, что степень инсайдерской угрозы определяется родом деятельности компании и ликвидностью информации, которая может стать предметом утечки. Больше всего утечек наблюдается в высокотехнологичных компаниях и медицинских учреждениях, при этом наиболее ликвидной является информация банков, финансовых учреждений, промышленных и коммерческих компаний.

Ключевые слова: корпоративная экономическая безопасность, человеческий капитал, кадровая безопасность, инсайдерская угроза, информационная база данных.

Введение

Традиционно кадровая безопасность как часть корпоративной экономической безопасности рассматривалась преимущественно в физических аспектах, таких как защита предприятия и персонала, физическая защита важных документов, соблюдение процедур и политик контроля доступа и др. Однако с развитием информационных технологий, стали появляться другие угрозы экономической и кадровой безопасности. Если процедуры физической безопасности уже отработаны, то у большинства компаний, особенно в России, еще нет достаточного опыта защиты информации в киберпространстве. Проблема инсайдерских угроз становится все более актуальной, так как компания может нести убытки не только из-за утечки информации о своих изобретениях, но и через судебные иски в случае кражи личной информации подрядчиков. Это стало особенно актуальным после вступления в силу весной 2018 года Общеевропейского общего регламента по защите данных (GDPR), который устанавливает размер санкций за нарушения правил защиты персональных данных граждан ЕС. Это означает, что для выхода на международные рынки российские компании должны иметь надлежащий уровень защиты не только конфиденциальной информации компании, но и данных о заказчиках, контрагентах и т.д. То, что в целом воспринимается как нормальное явление в России, может привести к огромным штрафам и судебным искам за рубежом. В частности, очень часто при увольнении сотрудник компании заби-

рает с собой базу клиентов или поставщиков, потому что в компании нет соответствующих процедур для предотвращения подобных действий. То, что в России остается только частной проблемой компании, на зарубежных рынках может обернуться санкциями, штрафами и потерей клиентов и партнеров. Именно поэтому инсайдерские угрозы и утечка информации становятся важной составляющей экономической и кадровой безопасности предприятия, особенно если его целью является выход на внешние рынки. Например, по данным международного аналитического центра InfoWatch, осуществляющего постоянный мониторинг утечки конфиденциальной информации, в 2018 году было зарегистрировано 2263 случая серьезной утечки конфиденциальной информации. Следует отметить, что компании и аналитические центры, исследующие и отслеживающие инсайдерские угрозы, не в состоянии охватить все случаи утечек, поэтому они фокусируются на крупнейших компаниях и крупных утечках, повлекших существенные негативные финансовые последствия для компаний. Так, по данным центра, в 2018 году в результате утечек было скомпрометировано более 7,28 млрд записей персональных данных (номера социального страхования, реквизиты банковских и других видов карт и пр.).

Цель статьи — проанализировать существующие методические подходы к защите от инсайдерских угроз на предприятии как составляющей кадровой и экономической безопасности.

Научная гипотеза состоит в том, что разные отрасли имеют разную уязвимость к инсайдерским угрозам и разные подходы к управлению инсайдерскими угрозами.

Методологической и информационной основой нашего исследования являются аналитическая информация и базы данных, предоставленные аналитическим центром InfoWatch.

Обзор литературы

В последнее время в научной литературе широкое распространение получил вопрос об инсайдерских угрозах и защите от них. Ученые стали активно обращать внимание на проблему утечки информации, а также на то, что она имеет не только внешние, но и внутренние источники.

В частности, по данным Agrafiotis et al. [1], угроза для организации со стороны собственных сотрудников продолжает неуклонно и значительно расти, о чем свидетельствует множество примеров. Авторы подчеркивают, что внутренние угрозы нельзя просто игнорировать. Они рассматривают технологии, которые можно использовать для автоматического обнаружения инсайдеров. Эти технологии должны выявлять угрозы, контролируя персонал для выполнения определенных действий. По мнению ученых, эти действия можно разделить на две категории: 1) действия, нарушающие политики, процедуры и регламенты, созданные специально для предотвращения поведения персонала, которое может представлять угрозу; 2) действия, аналогичные уже идентифицированным как инсайдерская атака. В частности, предлагается использовать так называемые «ловушки» в информационной системе, которые будут реагировать навышеуказанныедействияипредупреждатьобопасности.

Махаджан и Шарма [2] отмечают, что организации все чаще используют облачные технологии для хранения важной информации, поэтому они не в состоянии полностью контролировать процедуры безопасности и защиты. В своем исследовании авторы выделяют несколько типов облаков, которые компании могут использовать для хранения своей информации, а именно, частные, общие, общедоступные, гибридные облака, имеющие разную степень защиты. Также авторы выделяют две основные возможности: наличие инсайдера среди сотрудников компании, занимающейся предоставлением облачных услуг, и наличие инсайдера в другой компании, которая занимается организацией облачных услуг в рамках аутсорсинг. Авторы предлагают несколько возможных действий, которые могут выявить угрозу и нейтрализовать ее.

Важным аспектом, рассматриваемым в научной литературе, является выявление возможных методов обнаружения инсайдерских атак. В частности, Sanzgiri & Dasgupta [3] считают, что большинство инсайдерских атак осуществляется лицами, обладающими соответствующими техническими навыками, поэтому наиболее успешным является сочетание различных стратегий и методов их распознавания.

Конт и др. [4] попытались создать универсальную программу для обнаружения и распознавания инсайдерских угроз. С этой целью они выделили пять различных типов угроз (саботаж, кража, мошенничество, шпионаж и несчастный случай) и предложили шесть отдельных индикаторов, основанных на поведенческих и технических аспектах угрозы. По мнению авторов, одновременное использование всех индикаторов позволит минимизировать ущерб и в лучшем случае вообще предотвратить инцидент.

Ринг и др. [5] предложили новый алгоритм выявления инсайдерских угроз путем обнаружения аномальных помех в работе внутренней сети. Для повышения эффективности такого подхода авторы предлагают использовать исторические данные об инсайдерских атаках и анализ предшествовавших им действий во избежание ложных срабатываний.

Парк и др. [6] предложили использовать поведение сотрудников в социальных сетях для выявления возможных инсайдерских угроз. Авторы предложили алгоритм и критерии, по которым можно выявить потенциального инсайдера. Они пришли к выводу, что инсайдера можно выявить, проанализировав его посты в социальных сетях, при условии использования им определенного набора слов и словосочетаний, выражающих негативные эмоции и намерения.

В свою очередь, Элифоглу и соавт. [7] предложили повысить эффективность борьбы с инсайдерскими угрозами за счет более плодотворного взаимодействия подразделений управления информационными технологиями и управления персоналом. Они подчеркивают, что основными причинами инсайдерских атак являются ошибки, халатность, жадность или безрассудное поведение.

Эггеншвилер и др. [8] отметили, что фирмы, предоставляющие финансовые услуги, являются одними из наиболее уязвимых для инсайдерских атак, поскольку они приводят к огромным убыткам. Авторы сосредоточились не только на том, как фирмы обнаруживают атаки, но и на возможных способах реагирования на них. Они отметили, что финансовые фирмы используют два подхода: внутреннее и внешнее реагирование. Если, по их мнению, атака имела минимальные негативные последствия, то используется внутренний подход, т.е. проблема решается внутри фирмы для предотвращения огласки. И только в том случае, когда последствия невозможно скрыть, используется внешний подход, требующий привлечения третьей стороны к разрешению конфликта.

Abd & Hassan [9] считают, что защита коммерческой тайны является одним из важнейших направлений экономической безопасности компании и должна быть частью кадровой безопасности. По мнению исследователей, правовых мер недостаточно для надежной защиты информации, поэтому она должна сопровождаться соответствующими административными инструментами. Для этого авторы предлагают использовать пять основных методов: строгий набор, использование обязательного трудового договора, постоянное ознакомление сотрудников с политикой защиты информации компании, постоянный контроль за действиями сотрудников с информацией и применение адекватных ограничений, снятие всех документов, содержащих коммерческую тайну, у работника при увольнении.

Не менее важен вопрос потерь компании от инсайдерских угроз. При этом могут быть не только прямые убытки (стоимость похищенного изобретения, деньги, интеллектуальная собственность), но и косвенные затраты или так называемая «упущенная выгода». В большинстве случаев его очень сложно подсчитать, и существующие методы ориентированы главным образом на отдельные аспекты повреждения. Буткевичюс [10] предлагает универсальную модель расчета упущенной выгоды, которая учитывает структуру затрат компании и позволяет учесть максимально возможную прибыль, которую получила бы фирма, если бы не было утечки.

Результаты и обсуждение

Наш обзор литературы показал, что подавляющее большинство исследователей подчеркивают, что защита информации от внешних и внутренних угроз в цифровом пространстве становится приоритетом для компаний. В то время как большинство компаний уже внедрили эффективные процедуры для обеспечения физической безопасности и предприняли некоторые успешные попытки защитить информацию от внешних угроз, проблема предотвращения инсайдерских атак по-прежнему остается в значительной степени нерешенной.

Согласно исследованию Коста и др. [11], злоумышленник-инсайдер — это бывший или действующий сотрудник, подрядчик или деловой партнер, на которого распространяются следующие требования:

— имеет или имел авторизованный доступ к внутренней организационной сети системы или данным;
— умышленно превысил уровень доступа или использовал свой доступ таким образом, чтобы нанести вред конфиденциальности, целостности и доступности информации или информационной системы организации.

В результате на внутренние угрозы влияют технические, поведенческие или организационные проблемы, поэтому для их устранения необходимо разработать политики, процедуры и технологии.

Одной из первых задач при выявлении и предотвращении инсайдерской атаки является определение ее типа. Например, Уитти [12] выделяет следующие виды инсайдерских атак: мошенничество, отмывание денег, ущерб репутации, кража (в том числе кража IP-адреса, данных, аккаунта), нелегальное трудоустройство.

Внутренние угрозы могут быть результатом преднамеренных или случайных действий. Предотвратить случайные действия можно, главным образом, путем повышения осведомленности персонала о такой возможности, т.е. повышения его информационной грамотности. Вместо этого стратегия кадровой безопасности компании должна быть направлена на предотвращение умышленных действий.

При использовании информационных технологий для предотвращения утечки информации, как правило,

имеют место следующие действия, представляющие инсайдерскую угрозу, которые могут быть отслежены автоматически:

1. Физическая невозможность действий (например, вход с IP-адреса, географически не совпадающего с физическим местонахождением сотрудника, VPN-подключение с разных IP-адресов, географически удаленных, но принадлежащих одной учетной записи и т. д.);
2. Доступ к сайтам из черного списка;
3. Использование внешних накопителей, которые не авторизованы;
4. Многократные неудачные попытки входа в разные аккаунты;
5. Постоянная отправка по электронной почте файлов с именами, совпадающими с зарегистрированными в системе;
6. Постоянная отправка писем с большими файлами в приложении;
7. Чрезмерное использование социальных сетей в рабочее время;
8. Безвозвратное удаление файлов большого размера или с именами, зарегистрированными в системе.

Автоматическое отслеживание таких действий поможет выявить инсайдерские угрозы на ранней стадии и предотвратить дальнейшую утечку важной информации.

Исследование аналитического центра InfoWatch [13] показывает рост угрозы утечки информации, что приводит к убыткам компаний. В последнее время наблюдается стремительный рост числа таких случаев. В частности, количество утечек информации увеличилось с 801 случая в 2011 году до 2263 случаев в 2018 году. Особенно заметным был скачок в 2017 году (количество утечек увеличилось на 36,9 % (до 2131 случая) по сравнению с предыдущим годом (1556 случаев), тогда как в 2018 году рост был несколько умеренным (всего 6,1 %).

Что касается источника утечки информации, то в 2018 году большинство случаев (1393) (63 %) произошло по вине инсайдеров, тогда как на внешние атаки пришлось лишь 37 %.

Касаемо характера утекшей информации, попрежнему преобладают персональные данные (69,5 %), на втором месте платежная информация (16,9 %), на третьем — коммерческая тайна (8,1 %).

Следует отметить, что для компании важны все виды информации, так как они могут привести к потенциальным убыткам. Проблема в том, что потери от утечки коммерческой информации можно рассчитать и спрогнозировать. Убытки от утечки других видов информации не могут быть рассчитаны напрямую. Например, утечка персональных данных клиентов может привести к потере доверия к компании, судебным искам, штрафам, падению цен на акции и т.д., в зависимости от публичности инцидента. Можно сказать, что на данном этапе такие утечки становятся все более опасными для экономической безопасности компании.

Утечки также происходили по разным каналам. Приоритезация каналов инсайдерских угроз важна для разработки дальнейшей политики кадровой безопасности. Основными каналами остаются кража или потеря оборудования, мобильных устройств, съемных носителей, сети, электронной почты, бумажных документов, обмен информационными уведомлениями. В частности, лидером остается сеть Интернет (браузер или облачное хранилище) (72,2 % в 2018 г.), значительная доля приходится на электронную почту (8,0 % в 2018 г.) и бумажные носители (11,0 % в 2018 г.). Другими каналами утечки были мобильные устройства, съемные носители, потеря оборудования и обмен сообщениями, хотя их доля остается низкой.

Если рассматривать сферы деятельности, наиболее подверженные утечкам, то лидерами являются высокотехнологичные компании и медицинские учреждения.

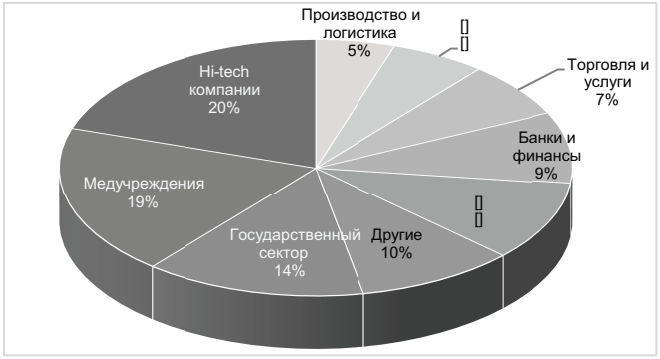

Рис. 1. Доли утечек по отраслям в 2018 г.

Такое распределение вполне естественно. Привлекательность отрасли определяется относительной ликвидностью данных, имеющихся у компаний в этом секторе. Злоумышленники нацелены на лёгкие деньги, поэтому выбирают наименее защищенные (в случае с медицинскими учреждениями) или наиболее ценные на рынке (для случая с Hi-tech компаниями) данные.

Заключение

Выводы. Утечки информации представляют серьезную угрозу экономической и кадровой безопасности компании. В настоящее время фирмы имеют значительные усовершенствования и эффективные процедуры противодействия внешним угрозам, однако защита от инсайдерских атак остается достаточно низкой. В ходе

исследования было определено понятие инсайдерского злоумышленника, установлены виды инсайдерских угроз, а также обозначены основные действия персонала перед инсайдерской атакой.

Определено, что степень инсайдерской угрозы определяется видом деятельности компании и ликвидностью информации, которая может стать предметом утечки. Больше всего утечек наблюдается в высокотехнологичных компаниях и медицинских учреждениях, при этом наиболее ликвидной является информация банков, финансовых учреждений, промышленных и коммерческих компаний.

В дальнейшем для определения уровня осведомленности российских компаний об инсайдерских угрозах предлагаем провести опрос среди руководителей подразделений безопасности или высших руководителей компаний России, отвечающих за информационную и кадровую безопасность, что позволит определить уровень инсайдерских угроз к экономической безопасности этих компаний.

ЛИТЕРАТУРА

1. Agrafiotis, I., Erola, A., Goldsmith, M., & Creese, S. (2017). Formalising Policies for Insider-threat Detection: A Tripwire Grammar. JoWUA, 8 (1), 26–43.
2. Mahajan, A., & Sharma, S. (2015). The malicious insiders threat in the cloud. International Journal of Engineering Research and General Science, 3 (2), 245–256.
3. Sanzgiri, A., & Dasgupta, D. (2016, April). Classification of insider threat detection techniques. Proceedings of the 11th annual cyber and information security research conference. (pp. 1–4).
4. Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.M. (2015). Insider threat detection study. NATO CCD COE. Tallinn.
5. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2017). A toolset for intrusion and insider threat detection. Data Analytics and Decision Support for Cybersecurity. Cham: Springer.
6. Park, W., You, Y., & Lee, K. (2018). Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media. Security and Communication Networks.
7. Elifoglu, I.H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. Review of Business, 38 (2), 61–73.
8. Eggenschwiler, J., Agrafiotis, I., & Nurse, J. R. (2016). Insider threat response and recovery strategies in financial services firms. Computer Fraud & Security, 11, 12–19.
9. Abd J., J., & Hassan, H. (2020). Protecting trade secret from theft and corporate espionage: some legal and administrative measures. International Journal of Business & Society, 21.
10. Butkeviþius, R. (2019). Universal Model of Lost Profits Calculation. Ekonomika (Economics), 98 (2), 97–111.
11. Costa, D.L., Albrethsen, M.J., & Collins, M.L. (2016). Insider threat indicator ontology (υ CMU/SEI-2016-TR-007). Pittsburgh: Carnegie-Mellon University, 2016.
12. Whitty, M.T. (2018). Developing a conceptual model for insider threat. Journal of Management & Organization, 1–19.
13. InfoWatch. (2019). A Stud on Global Data Leaks in 2018. infowatch.com. Retrieved from [Электронный ресурс]. — URL: https://infowatch.com/sites/default/files/report/analytics/ Global_Data_Breaches_2018.pdf. (дата обращения 01.04.2023).

Журнал «Современная наука: актуальные проблемы теории и практики»