Дарья Егоровна ДЕНИСКИНА
студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, d.e.deniskina@gmail.com
Юлия Сергеевна САХНО
кандидат экономических наук, доцент, доцент кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, y.s.sakhno@utmn.ru

УТЕЧКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БИЗНЕСА

Аннотация. Статья посвящена изучению утечки конфиденциальной информации, как угрозы экономической безопасности предприятия. Дано определение конфиденциальной информации, а также представлены классификация и ответственность. Были рассмотрены основные показатели за последние года, вектор воздействия и причины потери информации. Кроме этого, предложены рекомендации по совершенствованию мер защиты конфиденциальной информации от внутренних утечек.
Ключевые слова: конфиденциальная информация, экономическая безопасность, утечка информации, ответственность, внутренний нарушитель, персонал, защита информации, технические факторы.

Darya Egorovna DENISKINA
Student of the specialty "Economic security" Tyumen State University, Tyumen, d.e.deniskina@gmail.com
Yulia Sergeevna SAKHNO
Candidate of Economic Sciences, Associate Professor of the Department of Economic Safety, System Analysis and Control Tyumen State University, Tyumen, y.s.sakhno@utmn.ru

LEAKAGE OF CONFIDENTIAL INFORMATION AS A THREAT TO THE ECONOMIC SEFETY OF BUSINESS

Abstract. The article is devoted to the study of the leakage of confidential information as a threat to the economic safety of the enterprise. The definition of confidential information is given, as well as the classification is presented. The main indicators for the last years, the vector of impact and the reasons for the loss of information were considered. In addition, recommendations for improving measures to protect confidential information from internal leaks are proposed.
Keywords: confidential information, economic safety, information leakage, responsibility, internal violator, personnel, information protection, technical factors.

Под конфиденциальной информацией понимается — сведения определенного характера, не подлежащие огласке, доступ к которым ограничен федеральными законами РФ.

В соответствии с Указом Президента РФ № 188 «Об утверждении Перечня сведений конфиденциального характера», конфиденциальная информация делится на следующие виды:

- персональные данные;
- тайна следствия и судопроизводства;
- служебная тайна;
- профессиональная тайна;
- коммерческая тайна;
- сведения о сущности изобретения;
- личные дела осужденных [1].

Вышеперечисленная информация может попасть в руки к лицу, которое не имеет к ней доступа, в открытый доступ или к конкурентам. Это и является утечкой данных. Если организация все-таки столкнулась с такой ситуацией, ей не избежать негативных последствий. Например, таких, как судебные разбирательства, штрафные санкции, потеря деловой репутации и постоянных клиентов, выплаты компенсаций пострадавшим и даже банкротство. Все это может нанести колоссальный удар по экономической безопасности предприятия в целом.

Разглашение информации ограниченного доступа может повлечь дисциплинарную, административную и уголовную ответственность. В трудовом кодексе установлено, что за разглашение сведений конфиденциального характера работником, работодатель вправе возложить полную материальную ответственность на сотрудника (п. 7, ст. 243 ТК РФ), а также расторгнуть трудовой договор (п. 6, ст. 81 ТК РФ) [2].

Административная ответственность за разглашение конфиденциальной предусмотрена в ст. 13.14 КоАП РФ. Данный вид ответственности наступает, если были совершены действия, указанные раннее, но они не содержат признаков уголовного преступления (обман, шантаж, подкуп и т. д.). Размер наложения штрафа на граждан — 5000-10000 руб.; на должностных лиц — 40 000-50 000 руб.; на юридических лиц — 100 000-200 000 руб. [3].

В уголовном кодексе предусмотрена ответственность за получение и разглашение информации, которая составляет коммерческую, налоговую или банковскую тайну. Такой вид ответственности применяется в случаях, когда:

– сведения собраны незаконным способом (похищение документов, подкуп, принуждение и т. д.);

– сведения разглашены или использованы без согласия их владельца;

– получены и разглашены сведения группой лиц, повлекшие крупный ущерб или тяжкие последствия.

Мера наказания зависит от тяжести преступления. Например, если сведения были собраны путем подкупа, то может быть применен один из следующих видов наказаний: штраф до 500 000 руб., исправительные работы сроком до 1 года, принудительные работы сроком до 2 лет, лишение свободы до 2 лет [4].

Система экономической безопасность состоит из нескольких элементов, таких как финансовая, информационная, правовая, кадровая и технологическая безопасность [5]. Если информация ограниченного доступа утекает из компании, то это автоматически затрагивает все элементы экономической безопасности. Именно поэтому, стоит изучить утечку конфиденциальных данных по вектору воздействия, источники возникновения и др., чтобы понять проблему более детально и найти пути решения.

По данным экспертно-аналитического центра InfoWatch в 2020 г. было зарегистрировано 404 случая утечки сведений конфиденциального характера на территории Российской Федерации, что представлено на рисунке 1.

На рисунке 1 мы видим, что число утечек конфиденциальной информации за весь период возросло на 197 случаев (49,6%). А в 2020 г. возросло всего на 9 случаев (2,3%), по сравнению с предыдущим 2019 годом. Замедление темпов роста скорее всего стало следствием массового перехода персонала на удаленную работу. Контроль стал затруднен и многие случаи могли остаться незамеченными.

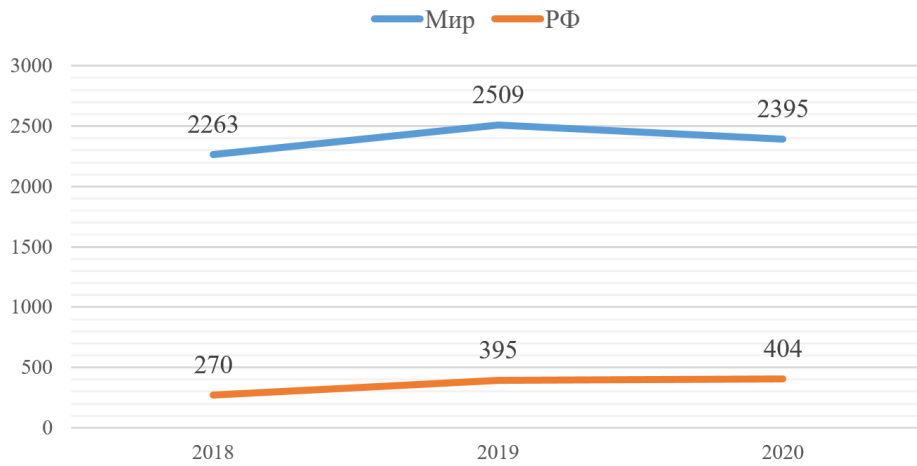

Рис. 1. Число утечек сведений конфиденциального характера
в Российской Федерации и мире в целом за период 2018-2020 гг.

Источник: составлено автором по данным [6].

Утечки данных могут произойти в результате действий внешнего или внутреннего нарушителя. Поэтому, далее рассмотрим распределение утечек данных по вектору воздействия на рисунке 2.

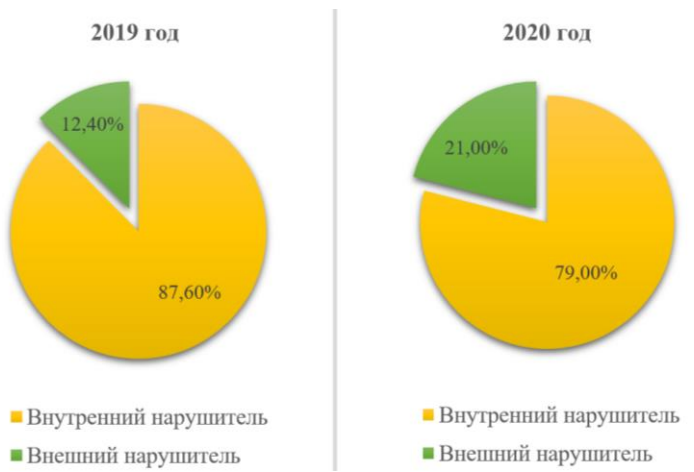

Рис. 2. Распределение утечек данных по вектору воздействия
в Российской Федерации за период 2019-2020 гг.

Источник: составлено автором по данным [6].

По данным, представленным на рисунке, можно сделать вывод, что в 2020 г. доля утечек информации по вине внешних нарушителей составила 21% от общего числа, что на 8,6% выше, чем в 2019 г. Но нельзя оставить без внимания тот факт, что доля внутренних нарушителей (сотрудников организаций) больше в разы и составляет 79% от общего числа.

Мы видим, что чаще всего, именно персонал разглашает конфиденциальную информация организации, в которой работает. Может быть такое, что сотрудники предприятий недостаточно осведомлены о работе с такой информацией, и их нарушения являются случайными. А возможно, какому-то сотруднику не нравится руководитель, он считает, что к нему относятся предвзято и таким образом решает отомстить, или же его могли подкупить конкуренты, которым утечка вашей информации будет только на руку. Для того чтобы разобраться случайны нарушения или же нет, рассмотрим распределение утечек данных по умыслу среди сотрудников предприятий на рисунке 3.

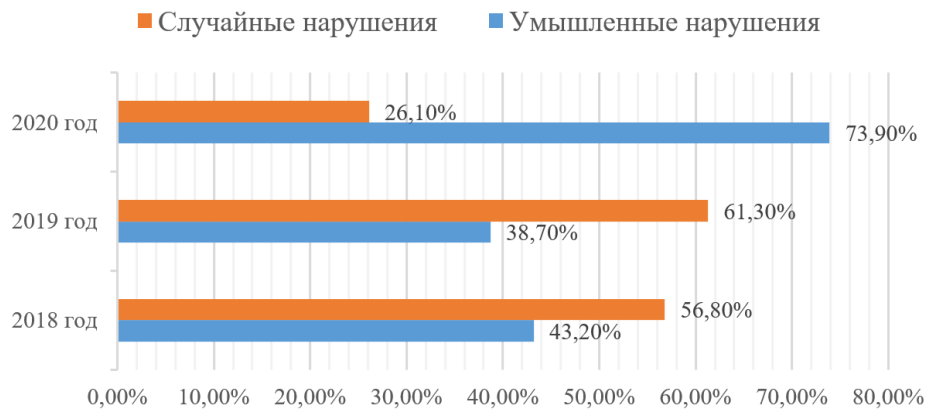

Рис. 3. Распределение утечек данных по умыслу среди сотрудников предприятий в Российской Федерации за период 2018-2020 гг.

Источник: составлено автором по данным [6].

Используя данные, представленные на рисунке 3, можно сделать вывод, что в 2018-2019 гг. доля случайных утечек была больше, чем доля преднамеренных. Чего не скажешь о показателях за 2020 г., где почти 74% случаев — умышленные действия сотрудников компаний. Данный факт может свидетельствовать о том, что цифровизация принесла нам не только новые возможности, но также и риски. Ведь сейчас на черном рынке конфиденциальная информация очень ценится и высоко вознаграждается. Кроме этого, мы можем сделать вывод, что предприятия стали намного лучше предупреждать случайные нарушения, т. к. до этого они были основной проблемой.

Далее целесообразно будет рассмотреть детальную картину утечек конфиденциальной информации по источникам возникновения, т. е. виновникам. Данная информация представлена на рисунке 4.

На рисунке 4 мы видим, что доля хакеров и неизвестных лиц составила 29,6% на 2020 г. Также четко прослеживается лидирующее положение непривилегированных сотрудников, даже несмотря на то, что их доля в 2020 г. сократилась по сравнению с 2019 г. на 10,4% и составила 59,8% среди всех источников утечек информации. Кроме этого, стоит отметить, что произошло увеличение случаев, когда виновным лицом является руководитель.

По рассмотренным данным, можно сделать вывод, что большая доля утечек конфиденциальной информации приходится на сотрудников предприятий. Во

всех рабочих процессах компании принимает участие персонал, следовательно, негативные последствия от внутренних утечек гораздо больше, чем от внешних. Чаще всего, внешние атаки нацелены на конкретные данные, к примеру, на персональные сведения пользователей. Когда работники могут скомпрометировать данные, которые являются для организации наиболее чувствительными [7]. Именно поэтому, мы хотим предложить рекомендации по совершенствованию мер защиты конфиденциальной информации от внутренних утечек.

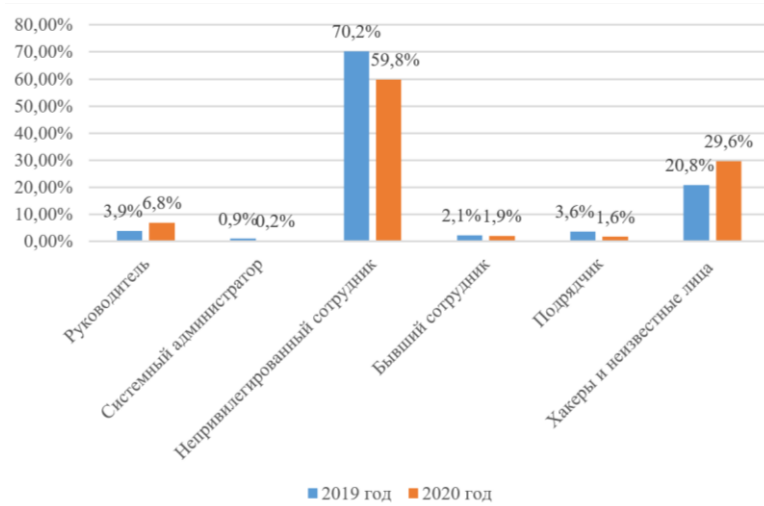

Рис. 4. Распределение утечек информации по источникам (виновникам) в Российской Федерации за период 2019-2020 гг.

Источник: составлено автором по данным [6].

Во-первых, стоит уделять должное внимание отбору персонала при приеме на работу. В организации должен быть отдел по набору кадров и их оценке, который занимается собеседованиями. Также стоит привлечь службу безопасности, которая в рамках своим компетенций проверит кандидата. Если должность, на которую претендует человек, заключает в себе работу с информацией ограниченного доступа, то в обязательном порядке подписывается соглашение о неразглашении конфиденциальной информации. Найм является самым первоначальным этапом, на котором можно избежать риска приема на работу недобросовестного сотрудника.

Во-вторых, стоит помнить, что каждый сотрудник в первую очередь человек, а не ресурс для достижения цели. Необходимо обеспечить качественную систему стимулирования, а также следует не оставлять без внимания внутренний климат коллектива. Взаимоотношения между сотрудниками, руководством должны быть доброжелательные и доверительные, чтобы работники даже и подумать не могли о нанесении вреда компании. Это стоит отслеживать, налаживать (если требуется) и поддерживать.

В-третьих, следует обеспечить обучение IT-культуре работников всех уровней. Необходимо проводить беседы с персоналом о важности кибербезопасности и организовать соответствующие обучающие тренинги по повышению осведомленности в сфере защиты конфиденциальной информации.

В-четвертых, рассмотрим техническую сторону. Для предотвращения несанкционированных утечек конфиденциальной информации в организациях следует применять межсетевые экраны, которые «блокируют» доступ на сторонние интернет-ресурсы. Кроме этого, программный комплекс класса DLP обеспечивает мониторинг сетевых действий сотрудников, проверяет все порты на компьютере и позволяет предупреждать копирование и перенос сведений на сторонние USB-устройства.

Таким образом, исходя из вышесказанного, можно сделать вывод, что почти 80% случаев утечки конфиденциальной информации происходят по вине сотрудников предприятия. Это является большой угрозой для экономической безопасности в целом, ведь персонал принимает участие во всех рабочих процессах компании. Именно поэтому, если соединить технические и человеческие факторы, то тогда организация будет способна обеспечить свою эффективную работу и должную защиту информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_13532/0179b6b5a612a4e6b17de579e3589aa0526bfe79/ (дата обращения: 24.03.2022).
2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 11.04.2022).
3. Разглашение информации с ограниченным доступом: Кодекс Российской Федерации об административных нарушениях от 30.12.2001 № 195-ФЗ // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_34661/835dca84f369ce440288da07465dbbf24791784a/ (дата обращения: 11.04.2022).
4. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну: Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/696074503229a6bf1978651f48895bf3a8831bd8/ (дата обращения: 11.04.2022).
5. Крохичева Г.Е., Архипов Э.Л., Виноградова М.А., Деточка Д.Е. Кадровая безопасность в системе экономической безопасности // Науковедение, 2016. № 3. С. 1-8. [дата публ. 30.04.2016]. URL: https://cyberleninka.ru/article/n/kadrovaya-bezopasnost-v-sisteme-ekonomicheskoy-bezopasnosti/viewer (дата обращения: 25.03.2022).
6. Россия: утечки информации ограниченного доступа, 2020 г. // Экспертно-аналитический центр InfoWatch: [сайт]. [дата публ. 06.07.2021]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/c_IW_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D1%8F_2020_%D1%83%D1%82%D0%B5%D1%87%D0%BA%D0%B8_v%201%207%201%D0%BF%D0%BF%20(2).pdf (дата обращения: 28.03.2022).
7. Назаров О.Г., Довыденко В.А. Утечка информации как угроза экономической безопасности предприятия // Экономика. Социология. Право, 2020. № 2. С. 28-33. [дата публ. 30.06.2020]. URL: https://cyberleninka.ru/article/n/utechka-informatsii-kak-ugroza-ekonomicheskoy-bezopasnosti-predpriyatiya/viewer (дата обращения: 02.04.2022).