**УДК 331.104**
**ББК 65.050**

**DOI: 10.25683/VOLBI.2020.53.416**

**Bulatenko Maria Andreevna**,
Candidate of Economics,
Senior Lecturer, Department of Financial Accounting and Control,
Institute for Integrated Security
and Special Instrument Engineering,
MIREA — Russian Technological University,
Russian Federation, Moscow,
e-mail: mabulatenko@gmail.com,
Researcher ID T-3499-2018, Scopus Author ID 57208481401,
ORCID 0000-0002-0017-1753

**Булатенко Мария Андреевна**,
канд. экон. наук,
старший преподаватель кафедры финансового учета и контроля,
Институт комплексной безопасности
и специального приборостроения,
МИРЭА — Российский технологический университет,
Российская Федерация, г. Москва,
e-mail: mabulatenko@gmail.com,
Researcher ID T-3499-2018, Scopus Author ID 57208481401,
ORCID 0000-0002-0017-1753

**Tarasova Nataliya Valentinovna**,
Candidate of Economics, Associate Professor,
Associate Professor, Department of Economic Expertise
and Financial Monitoring,
Institute of Integrated Security
and Special Instrument Engineering,
MIREA — Russian Technological University,
Russian Federation, Moscow,
e-mail: tais_n@mail.ru,
ORCID 0000-0002-5920-5807

**Тарасова Наталия Валентиновна**,
канд. экон. наук, доцент,
доцент кафедры экономической экспертизы
и финансового мониторинга,
Институт комплексной безопасности
и специального приборостроения,
МИРЭА — Российский технологический университет,
Российская Федерация, г. Москва,
e-mail: tais_n@mail.ru,
ORCID 0000-0002-5920-5807

# ПРИМЕНЕНИЕ ТЕХНОЛОГИИ АУТПЛЕЙСМЕНТА ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

# THE USE OF OUTPLACEMENT TECHNOLOGY TO INCREASE THE LEVEL OF ECONOMIC SECURITY OF THE ENTERPRISE

08.00.05 — Экономика и управление народным хозяйством
08.00.05 — Economics and national economy management

*В условиях современной экономики информация является одним из наиболее ценных активов компании, поэтому многие организации смещают акцент с обеспечения финансовой составляющей экономической безопасности на создание системы обеспечения информационной безопасности. При этом основное внимание уделяют технической стороне вопроса развития систем управления базами данными, забывая о том, что носителем любой ценной информации в организации является не только материальный объект, но и, в первую очередь, сотрудники организации. В статье собраны аналитические данные по утечке информации от работников на предприятии, демонстрирующие важность обеспечения кадровой составляющей экономической безопасности. Однако существующих показателей для мониторинга кадровой безопасности явно недостаточно. Статистические данные свидетельствуют о том, что увольняющиеся и увольняемые сотрудники — особая категория риска с точки зрения безопасности конфиденциальной информации, следовательно, и экономической безопасности предприятия. Даже при условии наличия развитой системы обеспечения информационной безопасности управлять поведением сотрудников после их увольнения из организации невозможно, а следовательно, угрозы экономической безопасности со стороны бывших сотрудников будут только усиливаться с возрастанием объема коммерчески ценной информации. В статье рассматриваются вопросы ответственности за разглашение коммерческой тайны работниками, уже не состоящими в трудовых отношениях с работодателем, но при этом факты утечки информации уже будут зафиксированы. В целях обеспечения экономической безопасности компании важно не допустить распространение ценной информации, которой обладают сотрудники организации после их увольнения. Поэтому авторами статьи предлагается обратить внимание на технологию аутплейсмента, или «вежливого» высвобождения персонала, для разработки кадровой службы организации комплекса превентивных мероприятий по обеспечению информационной и экономической безопасности компании.*

*In the current economy, information is one of the most valuable assets of the company so many organizations shift their focus from providing the financial component of economic security to creation of the information security system. At the same time, the main attention is paid to the technical side of development of the database management systems, forgetting that the carrier of any valuable information in the organization is not only a material object, but, first of all, the organization's employees. The article contains analytical data on information leakage from employees at the enterprise, demonstrating the importance of ensuring the human resources component of economic security. But the existing indicators of monitoring personnel security are clearly not sufficient. Statistics show that employees leaving the work place and dismissed are a special risk category from the point of view of security of confidential information, and therefore, of the economic security of enterprise. Even if there is a developed system for ensuring information security, it is impossible to control behavior of employees after*

*they are dismissed, and, therefore, threats to economic security on the part of former employees will only increase with increasing volume of commercially valuable information. The article discusses the issues of liability for disclosure of trade secrets by employees who are no longer in labor relations with the employer, but the facts of information leakage will already be recorded. In order to ensure the economic security of the company, it is important to prevent the dissemination of valuable information that employees of the organization possess after their dismissal. Therefore, the authors of the article propose to pay attention to the technology of outplacement, or "polite" release of personnel, to develop a personnel service for organizing a set of preventive measures to ensure the information and economic security of the company.*

*Ключевые слова: экономическая безопасность, кадровая безопасность, аутплейсмент, информационная безопасность, угрозы экономической безопасности, коммерческая тайна, утечка информации, персонал, лояльность сотрудников, угрозы со стороны сотрудников.*

*Keywords: economic security, personnel security, outplacement, information security, threats to economic security, trade secrets, information leakage, personnel, employee loyalty, threats from employees.*

## Введение

В современных условиях политической и финансовой нестабильности вопросы экономической безопасности обретают все большую значимость в управлении ресурсами организаций. Взаимосвязь таких системообразующих факторов, как информация и персонал, несет в себе целый спектр перспектив развития, но и возможных проблем. Без использования современных методов в управлении этими ресурсами добиться успеха, стабильного и безопасного развития не представляется возможным. Все эти аспекты определяют **актуальность** рассматриваемой темы.

**Изученность проблемы.** Вопросы экономической безопасности организаций, анализа и оценки ее уровня рассматривались российскими и зарубежными исследователями в последние десятилетия достаточно активно, например Л. И. Абалкиным, А. Е. Городецким, Н. П. Купрещенко, В. К. Сенчаговым и др.

Влияние информации и технологий на деятельность предприятий также изучалось в многочисленных трудах ученых и специалистов, таких как А. М. Карминский, Б. В. Черников, Е. П. Бочаров, Г. Н. Смирнова, Дж. Кантер и др.

Труды Е. В. Маслова, В. А. Спивакова, Е. И. Кудрявцевой и других исследователей позволяют сформировать представление о методах управления и развития персонала как одного из значимых ресурсов в деятельности экономических субъектов.

Однако исследованию влияния взаимосвязи таких ресурсов, как информация и персонал, на экономическую безопасность уделено мало внимания.

**Целесообразность разработки темы** авторы видят в том, что научный интерес предлагаемой темы возникает в связи с необходимостью обеспечения экономической безопасности компании, и важным является не допустить распространение ценной информации, которой обладают сотрудники организации после их увольнения.

**Научная новизна** заключается в развитии частных технологий управления персоналом в целях обеспечения экономической безопасности компаний.

**Цель** исследования заключается в теоретическом обосновании и практическом анализе применения технологии аутплейсмента для укрепления экономической безопасности компаний.

Для достижения поставленной цели были решены следующие **задачи**:

– проанализированы виды утечек корпоративной информации;

– рассмотрены возможности применения технологии аутплейсмента в системе обеспечения экономической безопасности хозяйствующих субъектов.

**Теоретическая и практическая значимость** работы заключается в расширении теоретико-прикладных знаний и их систематизации для укрепления экономической безопасности компаний посредством применения технологии аутплейсмента.

## Основная часть

Целенаправленная деятельность по обеспечению экономической безопасности предприятия чаще всего ассоциируется с эффективным управлением денежными потоками, но это только ее финансовая составляющая. В современных условиях все большее внимание уделяется информационной безопасности, однако и в данном направлении преобладает технический аспект. Управление предприятием, включая обеспечение экономической безопасности, в первую очередь связано с работой с людьми. И здесь необходимо учитывать, что угрозы от сотрудников являются специфическими и требуют особых подходов.

По свидетельству статистики [1], до 80 % потерь и утрат репутации организации могут быть связаны с ее персоналом. Именно потому актуальным аспектом является внимание к кадровой безопасности. Компетентные действия руководителя позволят снизить убытки организации, связанные с ее персоналом.

Как известно, для оценки уровня экономической безопасности предприятия применяются различные методы: индикативный, ресурсно-функциональный, увеличения стоимости бизнеса, эффективности использования собственного капитала и др.

Ресурсно-функциональный метод предполагает оценку различных функциональных критериев деятельности предприятия и сведение их в один интегральный критерий экономической безопасности с учетом ущерба и без учета ущерба, который мог быть причинен предприятию [2].

В экономической литературе [2, 3] чаще всего выделяется семь основных функциональных составляющих экономической безопасности предприятия (табл. 1).

Служба экономической безопасности делегирует часть своих задач на другие отделы предприятия, в частности задачи по мониторингу и снижению потенциальных и реальных угроз со стороны сотрудников организацию передаются отделу по управлению персоналом. Именно там должна обеспечиваться основа кадровой безопасности предприятия: компетентный подбор кадров, обучение и мотивация работников, а также грамотное использование человеческих ресурсов. Все меры должны быть зафиксированы в кадровой политике.

*Таблица 1*

**Функциональные составляющие экономической безопасности предприятия**

| Составляющие экономической безопасности предприятия | Факторы экономической безопасности предприятия |
|---|---|
| Финансовая | Финансовая устойчивость, долговые обязательства, собственный капитал, инвестированный капитал, эффективность использования ресурсов и т. п. |
| Интеллектуально-инновационная | Инновационная составляющая в выручке предприятия, эффективность инноваций |
| Кадровая | Текучесть кадров, вооруженность труда и фондоотдача, оплата труда и выручка от одного рубля оплаты труда, производительность труда |
| Производственно-технологическая | Определение потребности в оборотных и основных средствах, эффективность их использования, износ производственных фондов |
| Правовая | Владение, распоряжение и управление материальными и нематериальными активами, право владения и использования программных продуктов, товарных знаков, ноу-хау, марки научного опыта и др. |
| Экологическая | Расходы на экологические мероприятия, выполнение экологических стандартов, штрафы, пени и другие платежи |
| Информационная | Факторы скорости реагирования на изменение внешней среды |
| Силовая | Факторы эффективности функционирования собственной системы безопасности |

Значительный ущерб организации могут нанести как умышленные негативные действия сотрудников (внутренние угрозы кадровой безопасности), так и непреднамеренные действия сотрудников, не зависящие от их воли и сознания (внешние угрозы). Примеры внутренних и внешних угроз кадровой безопасности приведены в табл. 2 [4].

*Таблица 2*

**Внешние и внутренние угрозы кадровой безопасности**

| Внешние угрозы | Внутренние угрозы |
|---|---|
| Наличие у конкурентов более эффективной мотивационной системы.<br>Присутствует внешняя зависимость от сотрудников организации.<br>Конкурентные предложения для квалифицированных работников.<br>Активность инфляционных процессов, что необходимо учитывать при оплате труда | Неграмотная организация корпоративной политики.<br>Несоответствие квалификационных требований к занимаемой должности.<br>Непрофессиональный отбор и увольнение сотрудников.<br>Посредственная организация системы обучения или полное ее отсутствие.<br>Плохо налаженная система мотивации |

В кадровом направлении можно выделить несколько областей: подбор и отбор персонала, вопросы мотивации, корпоративной культуры, адаптации. Только обучение, организатором которого является служба персонала, чаще всего не связано с безопасностью, за исключением курсов или предметов, касающихся охраны труда, предотвращения рисков, пожарной безопасности.

В части интеллектуальной и кадровой безопасности специалистам по работе с персоналом необходимо учитывать как внешние, так и внутренние угрозы со стороны сотрудников и организовать такую систему управления кадровыми ресурсами, при которой будет обеспечена не только квалифицированная проверка кандидатов для приема на работу, но и контроль лояльности персонала, исключающий его вербовку со стороны конкурентов. Для этого целесообразно своевременно актуализировать мотивационные программы, включать в них поощрение активности сотрудников и развивать интеллектуальный потенциал предприятия посредством современных обучающих курсов. Весьма действенным, но не поддерживаемым корпоративной культурой многих российских организаций, механизмом экономической безопасности предприятия является пропаганда «стукачества» и «доносительства», посредством которых руководитель сможет своевременно получать информацию о злоупотреблениях служебными полномочиями со стороны подчиненных и пресекать данные возможности, не дожидаясь, пока организации будет нанесен значительный ущерб.

Общее состояние безопасности организации зависит от ключевых показателей экономической безопасности, определяющих эффективность работы персонала [2]:

1) производительность труда — также может называться результативность труда, — показывающая либо выработку одного сотрудника, либо трудоемкость единицы продукции (товара или услуги);

2) средняя заработная плата по организации в целом и по уровням управления (средний показатель региональный или среднеотраслевой уровень) и децильный коэффициент;

3) соотношение темпов роста производительности труда и средней заработной платы;

4) текучесть кадров, характеризующая степень удовлетворенности работников предприятия и социальную защищенность.

Профессиональная и возрастная структура персонала, средний стаж работы сотрудников и другие компоненты структуры могут служить информацией для анализа качества сотрудников, их удовлетворенности работой.

С точки зрения экономической безопасности при работе с персоналом необходимо учитывать, что такая очевидная мера повышения эффективности труда у сотрудников, как повышение заработной платы и другие материальные поощрения, без соответствующих темпов роста выручки приведут только к снижению показателей финансовой безопасности организации (например, рентабельности продукции или продаж). Основное внимание в сфере кадровой безопасности должно быть

сосредоточено на повышении лояльности сотрудников без увеличения зарплатоемкости продукции.

Под лояльностью персонала понимают надежность, профессиональную пригодность, приверженность целям компании, наличие или отсутствие нежелательных действий и злоупотреблений: пьянства, утечки информации, хищений и т. п.

Неудовлетворенность условиями труда, заработной платой, принципами управления, отсутствие системы адаптации новичков ведет к большому числу увольнений. Высокая текучесть персонала связана с экономическим ущербом для компании — это потери от простоя производства, затраты на поиск и обучение нового персонала, снижением продуктивности у тех, кто собрался увольняться, и новичков, высокий процент брака, высокие риски финансовых потерь и конфиденциальности.

Обычно самая большая текучесть кадров наблюдается среди категории работающих, чей стаж в компании составлял менее двух лет. Данный показатель является значимым и его необходимо анализировать:

1. Показатель компании сравнивают со средним по отрасли и категории сотрудников. Например, в торговле нормальным уровнем текучести считают 30…40 % в год. Отличаются нормальные показатели текучести кадров и для различных категории сотрудников. Для топ-менеджеров это не более 2 %, для неквалифицированных работников — 30…50 %.

2. Проводят мониторинг показателя текучести по подразделениям компании за последние 3—5 лет, а также за наиболее успешный период и сравнивают с данными настоящего периода.

Служба безопасности дает оценку того, как следующие факторы повлияли на лояльность и количество увольнений сотрудников:

1) смена руководства подразделения/топ-менеджмента;

2) изменения в системе оплаты труда;

3) изменения в условиях работы — переезд в новый офис, существенное расширение штата без аренды дополнительных площадей, условия охраны труда в производственных цехах;

4) улучшение или ухудшение финансового положения компании;

5) настроения на рынке труда в регионе (в небольшом городе открылось крупное производство, ведущий банк перевел в регион свой колл-центр и т. д.);

6) активность хедхантеров конкурентов и др.

Чтобы исключить проблемы с лояльностью, служба безопасности организует:

1) проверку кандидатов на вакансии;

2) согласование со службой безопасности внутренних перемещений, повышений из линейного персонала;

3) при увольнении по критически важным должностным позициям — обязательное интервью специалиста службы безопасности с увольняющимся сотрудником.

Лояльные сотрудники не создают проблем службе безопасности.

Службе безопасности необходимо выработать подходы к управлению лояльностью персонала в зависимости от масштабов потенциального риска:

1. Должности максимального риска, на которых нелояльный сотрудник может нанести непоправимый ущерб компании. Прежде всего это топ-менеджмент. Сотрудники, которые заняты охраной руководства, владеют клиентской базой, технологическими и финансовыми секретами, иной ценной конфиденциальной информацией, должны проявлять высокие показатели активной лояльности. Важно присмотреться и к другим звеньям, например к корпоративному программисту, секретарю директора или бухгалтеру-казначею с доступом к электронным ключам от всех расчетных счетов компании. По отношению к должностям максимального риска разрабатывают более развернутый план мониторинга и повышения лояльности.

2. Должности умеренного риска, которые сопряжены с доступом к фрагментарной информации. Утечка, преждевременное раскрытие такой информации из-за нелояльных действий сотрудника не нанесут непоправимый ущерб, но затормозят и осложнят достижение стратегических целей компании. К данной группе принято относить линейный менеджмент, руководителей отделов и проектов, ведущих специалистов.

3. Должности низкого риска — рядовые сотрудники, рабочие в цехах, обслуживающий персонал. Эти категории персонала не обладают конфиденциальной информацией и уникальными навыками. Уход их из компании, как правило, не наносит вреда и не вызывает серьезных негативных последствий. Ошибкой службой безопасности будет не заниматься повышением лояльности работников низкого риска. Активная деловая разведка конкурента с участием сотрудников, которые определены в категорию низкого риска, может нанести значительный ущерб компании.

В условиях современной экономики информация является одним из наиболее ценных активов компании. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ относит к конфиденциальной информации любые сведения, доступ к которым ограничен законодательством, в частности персональные данные, информацию, составляющую профессиональную (адвокатскую, банковскую, аудиторскую и пр.), коммерческую, служебную и государственную тайну [5].

В коммерческих организациях законом охраняются персональные данные и коммерческая тайна, при этом от работодателя требуется соблюдение ряда условий, описанных в ч. 1 ст. 10 Закона о коммерческой тайне [6], а именно установление режима коммерческой тайны.

«Информация, составляющая коммерческую тайну, — это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны» [6].

Все чаще компании сталкиваются с необходимостью защиты своих прав в спорах с бывшими работниками, которые после увольнения унесли с собой коммерчески ценную информацию, например базу клиентов, наработки компании, пароли от баз данных и ключи доступа к управлению банковскими счетами, и стали использовать ее в собственных целях (множество подобных практических примеров можно найти в открытых СМИ [7—9]).

Увольняющиеся и увольняемые сотрудники — особая категория риска с точки зрения безопасности конфиденциальной информации, а следовательно, и экономической безопасности предприятия. Работники, покидая организацию, руководствуются разными мотивами и могут перед уходом поступить непорядочно по отношению к работодателю: модифицировать или уничтожить важные информационные активы, сохранить за собой неправомерный доступ, предоставить конфиденциальную информацию конкурентам компании или другим заинтересованным лицам, неправомерно скопировать доступные данные для дальнейшего использования в своих целях.

В стандарте Банка России СТО БР ИББС-1.0-2014 [10] отмечается, что наибольшими возможностями для нанесения ущерба организации обладает собственной персонал при нецелевом использовании предоставленного ему служебного доступа к информационным активам.

По результатам проведенного исследования, аналитиками компании Ernst & Young Global Limited [11] было установлено, что 88 % утечек данных российских пользователей случаются по вине сотрудников компаний, запрашивающих эти данные и в большинстве случаев стоимость данных (при продаже на черном рынке) сопоставима со средней заработной платой сотрудников, которые с ними работают.

Аналитический центр компании «СерчИнформ» опубликовал результаты ежегодного исследования уровня информационной безопасности в компаниях России и мира за 2018 г. [12]:

1) в 74 % случаев утечки информации от работников на предприятии виновны рядовые сотрудники, из них 25,5 % приходится на менеджеров отдела снабжения, 24 % на экономистов и 16,2 % на помощников руководителей (секретарей);

2) 29 % случаев утечки информации связаны с данными о клиентах и сделках, 24 % с технической информацией, 20 % с персональными данными (рис. 1);

3) свыше 30 % опрошенных сотрудников выражают готовность перейти на работу к конкурентам с большей зарплатой при условии передачи последним конфиденциальных данных бывшего работодателя.

Согласно результатам исследования Международного кадрового портала hh.ua, большинство сотрудников (порядка 76 %) считают, что авторские права на готовые материалы имеют и сотрудник, и компания в равной степени. Еще 11 % опрошенных считают, что все созданное когда-либо одним сотрудником должно находиться в его личном распоряжении. Именно поэтому, как показало исследование, больше половины сотрудников (56 %) забирают с собой рабочие материалы и корпоративные данные при увольнении [13].

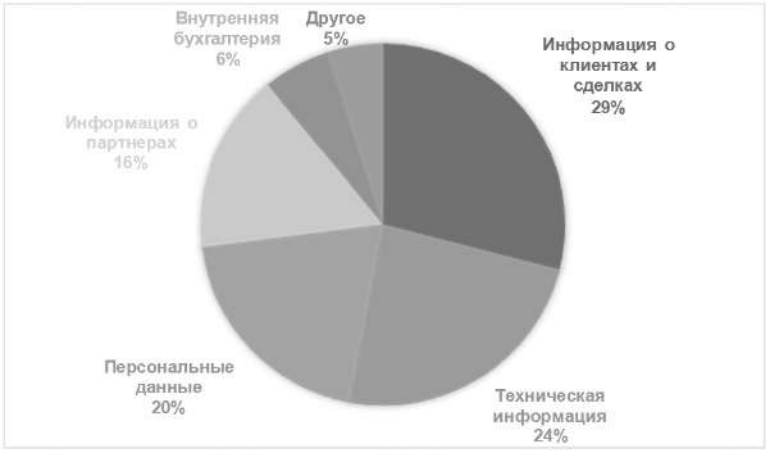


*Рис. 1.* Тип данных, скомпрометированных сотрудниками предприятий

Аналитический центр компании InfoWatch опубликовал результаты ежегодного исследования инцидентов в области информационной безопасности, связанных с действиями увольняющихся или увольняемых сотрудников государственных организаций и коммерческих компаний [14]:

1) 82,6 % деструктивных действий увольняющихся сотрудников в отношении корпоративной информации приходится на неправомерное копирование;

2) в 64,7 % случаев деструктивных действий увольняющихся сотрудников бывшим работодателем был зафиксирован прямой ущерб;

3) 53 % нарушителей решили воспользоваться ценной информацией работодателя в последний день работы в компании;

4) 58,8 % данных, которые неправомерно использовали уволившиеся сотрудники, составляли коммерческую тайну (рис. 2);

5) 42,8 % бывших сотрудников использовали ценные информационные активы своих работодателей в личных целях для карьерного роста на новом месте или реализации собственного бизнеса (рис. 3).

Таким образом, статистические данные свидетельствуют о том, что с уволенными сотрудниками необходимо работать. В зарубежной корпоративной культуре набирает популярность технология «вежливого» высвобождения персонала, так называемый аутплейсмент (англ. *outplacement*; от *out* — «вне» и *placement* — «определение на должность») — термин в менеджменте и управлении персоналом, связанный с деятельностью работодателя по трудоустройству увольняемых сотрудников [15].

Данная технология представляет собой своего рода программу помощи увольняемым сотрудникам, в которую входит ряд услуг, предоставляемых компанией в процессе расторжения трудового договора, а именно:

1) оплата услуг кадровых агентств по оценке специалиста и составления квалифицированного резюме, включая написание рекомендаций и сопроводительных писем;

2) оплата услуг консалтинговых фирм для проведения индивидуальных консультаций по поиску работы и успешному прохождению собеседования;

3) оплата услуг, связанных с оказанием психологической поддержки и проведением тренингов личностного роста, и др.

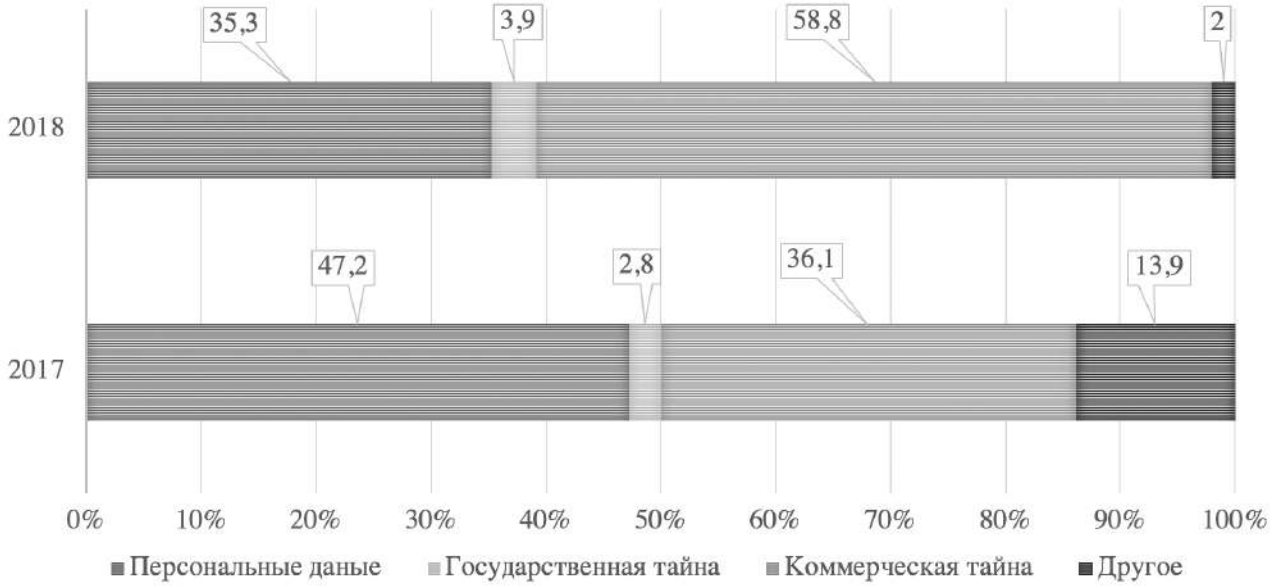


*Рис. 2.* Тип данных, скомпрометированных увольняющимися сотрудниками

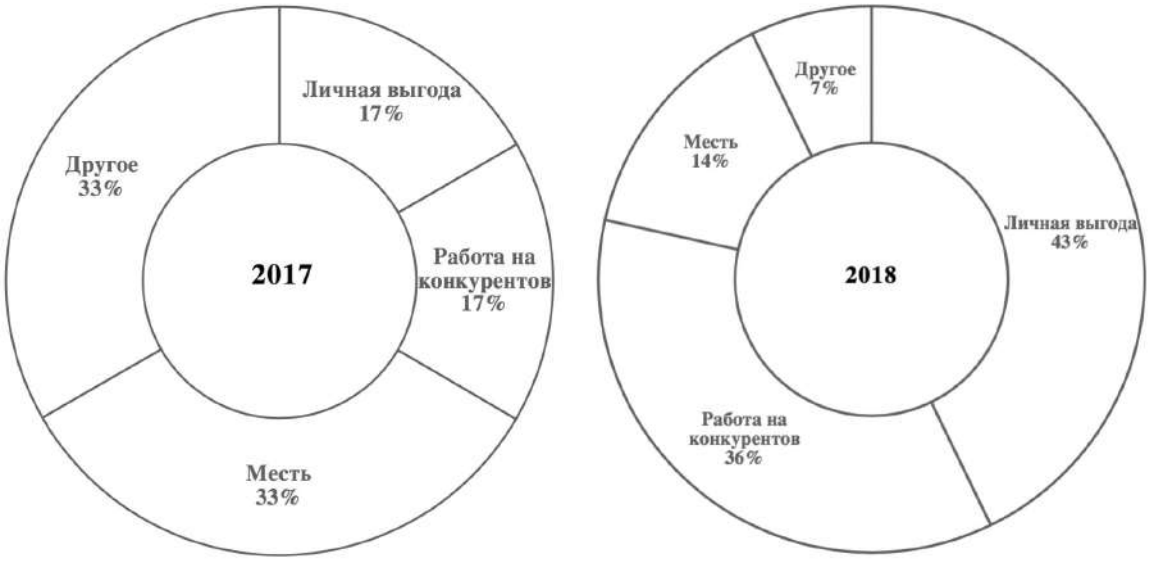


*Рис. 3.* Мотивы уволенных сотрудников, совершающих неправомерные действия с конфиденциальной информацией

При этом уволенному сотруднику ничего платить не приходится. Проводя такие мероприятия, компания демонстрирует заботу о своих сотрудниках, даже о тех, которые уже уволены. Таким образом, аутплейсмент повышает не только репутацию организации в глазах общественности, но и лояльность бывших сотрудников (позволит избежать ситуаций, когда уволенный сотрудник «затаит зло» на своего бывшего работодателя), что, в свою очередь, минимизирует возможные угрозы экономической безопасности со стороны только что выбывшего сотрудника.

Практика применения аутплейсмента предоставит возможности организации:

1) уменьшить количество судебных разбирательств по трудовым спорам;

2) повысить эффективность передачи дел бывшего сотрудника и сократить время на адаптацию нового сотрудника;

3) снизить компенсационные выплаты при увольнении (сокращении) персонала;

4) предупредить возможные утечки конфиденциальной информации о компании, а также разглашения уволенным сотрудником коммерческой тайны;

5) поддержать имидж социально-ориентированной компании на рынке труда, повысить репутацию организации среди персонала, тем самым обеспечив лояльность работающих сотрудников.

В западных крупных компаниях аутплейсмент является обычной практикой в случаях сокращения штата в связи с кризисом или реструктуризацией организации. В России культура увольнения, скорее, отсутствует, чем выражена хоть как-то. В нашей стране и увольняемые работники, и работодатели больше озабочены соблюдением буквы закона, нежели созданием перспективы на будущее (так как в случае несоблюдения формальностей хорошую перспективу может

получить длительное судебное разбирательство). Внедрять инструменты цивилизованного аутплейсмента нашему бизнес-сообществу еще только предстоит.

Опросы российских организаций демонстрируют, что аутплейсмент в России — достаточно редкое явление, в Москве его предоставляют 29 компаний, в Санкт-Петербурге — 13, в Нижнем Новгороде — 7, в Екатеринбурге и в Тюмени — всего 3 компании [5].

Очевидные положительные черты применения процедуры аутплейсмента могут быть омрачены только одним недостатком — необходимостью финансирования, однако повышение уровня экономической безопасности организации в полной мере компенсирует подобные затраты.

Таким образом, в практике работы с увольняемыми сотрудниками целесообразно использовать элементы технологии аутплейсмента:

1) обязать кадровую службу незамедлительно докладывать в службу безопасности об увольнении ключевых сотрудников, вне зависимости от причины и количества дней отработки;

2) предложить уходящему ключевому сотруднику стать консультантом для вашей компании, оказывать услуги по отдельным заявкам. Сотрудник переходит в новую компанию, но становится вашим консультантом, аутсорсером, подрядчиком;

3) проводить интервью с увольняющимися. Как правило, с людьми, которые покидают компанию, разговаривает непосредственный руководитель. Служба безопасности редко проводит беседы с этой категорией персонала. Тем не менее получать информацию о причинах увольнения необходимо. Если служба безопасности не имеет возможности говорить с каждым, то нужно ограничиться хотя бы беседой с ключевыми сотрудниками: руководителями, специалистами. Кроме того, во многих организациях менеджеры по персоналу проводят выходное интервью и фиксируют результаты. Сотруднику службы безопасности необходимо иметь доступ к таким данным;

4) изучать отзывы в социальных сетях. Многие бывшие сотрудники оставляют сообщения на сайтах отзывов и личных страницах, встречается и огромное количество анонимных комментариев. С авторами наиболее интересных посланий есть смысл знакомиться ближе и уточнять информацию.

Важным моментом является и то, что при правильном введении режима коммерческой тайны можно привлечь к материальной ответственности и уволенного сотрудника, если разглашение информации произошло в течение действия данного режима (ч. 4 ст. 11 [6]). При этом необходимо учитывать, что для привлечения работника к ответственности, помимо доказательств применения необходимых мер защиты, потребуется подтвердить и сам факт разглашения (п. 9 ст. 3 [6]).

Так, в практике судов признаются разглашением такие действия, как:

1) направление конфиденциальной информации сотрудником на личную почту (Определение Московского городского суда от 20 октября 2014 г. по делу № 4г/9-9007/2014);

2) передача пароля доступа к программному обеспечению, содержащему конфиденциальную информацию (Определение Московского городского суда от 16 октября 2014 г. по делу № 33-35077/201);

3) ненадлежащее хранение и утилизация конфиденциальной информации, ее носителей (Определение Московского городского суда от 19 августа 2014 г. № 4г8-7847);

4) сохранение работником конфиденциальной информации на USB-носителе (Определение Московского городского суда от 8 октября 2013 г. по делу № 11-33789).

Что касается гражданско-правовых отношений, то предустановленный в соглашении штраф является достаточно распространенной практикой. Закон позволяет привлечь к ответственности и работника, уже не состоящего в трудовых отношениях с работодателем и разгласившего его коммерческую тайну. В частности, работодатель вправе потребовать от нарушителя возмещения убытков, причиненных разглашением информации (ч. 4 ст. 11 Закона о коммерческой тайне).

**Заключение**

Таким образом, можно сделать вывод о том, что привлечение к ответственности за нарушение режима коммерческой тайны уволенного сотрудника также требует от организации мониторинга и дополнительного отвлечения финансовых средств. Но здесь необходимо учитывать еще и тот факт, что сотрудники могут обладать и другой ценной информацией, которая по тем или иным причинам не была отнесена к коммерческой тайне организации, а следовательно, после увольнения это также увеличивает угрозы экономической безопасности компании. Аналитические данные, представленные в статье, подтверждают, что такие риски существуют, а применяемые в службах безопасности (включая кадровый отдел) ключевые показатели эффективности не позволяют их оценить. В связи с этим целесообразно внедрить в корпоративную культуру организаций предложения авторов статьи о применении элементов технологии аутплейсмента. Такие превентивные мероприятия позволят снизить угрозы экономической безопасности со стороны увольняемых сотрудников.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Информационная безопасность для профессионалов. URL: https://www.anti-malware.ru.

2. Сергеев А. А. Экономическая безопасность предприятия : учеб. и практикум для вузов. М. : Юрайт, 2019. 273 с.

3. Хорев А. И., Шереметов А. Ю., Баркалова И. И. Ресурсно-функциональный подход как метод обеспечения экономической безопасности предприятия // Экономика. Инновации. Управление качеством. 2016. № 4(17). С. 76—78.

4. Коваленко Т. В., Гринченко Е. В. Кадровая безопасность как элемент экономической безопасности предприятия // Инновационные технологии в машиностроении, образовании и экономике. 2017. № 3(5). С. 19—22.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61798.

6. Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_48699.

7. Расстались по-плохому. Как бывшие сотрудники осложняют компаниям жизнь // РБК. Газета. 2016. 28 ноября (№ 221). URL: https://www.rbc.ru/newspaper/2016/11/29/582dbbb99a7947a46c6ca65b.

8. 15 сюрпризов от уволенного сотрудника: как работодателю к ним подготовиться. URL: https://vc.ru/flood/14245-15-bad-employees.

9. Комсомольчанку подозревают в мошенничестве в кредите // Аргументы и факты — Дальинформ. 2018. 29 декабря. URL: https://hab.aif.ru/incidents/komsomolchanku_podozrevayut_v_moshennichestve_na_kredite.

10. СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения (принят и введен в действие Распоряжением Банка России от 17.05.2014 г. № Р-399). URL: https://cbr.ru/Content/Document/File/46921/st-10-14.pdf.

11. Отчет Ernst & Young Global Limited. Развитие цифровой идентификации. URL: https://www.ey.com/Publication/vwLUAssets/ey-digital-id-survey-rus/$FILE/ey-digital-id-survey-rus.pdf.

12. Исследования уровня информационной безопасности в компаниях России и мира за 2018 год. URL: https://searchinform.ru/uploads/sites/1/2019/03/research2018-searchinform.pdf.

13. Увольнение сотрудника приводит к утечке информации. URL: http://www.ukpz.com.ua/uvolnenie-sotrudnika-privodit-k-utechke-informacii.

14. Исследование инцидентов информационной безопасности, связанных с действиями увольняющихся сотрудников, 2018 год. URL: https://www.infowatch.ru/resources/analytics/reports/17083.

15. Что такое аутплейсмент персонала в России: виды, этапы и методы. URL: https://kakzarabativat.ru.

**REFERENCES**

1. *Information security for professionals.* (In Russ.) URL: https://www.anti-malware.ru.

2. Sergeev A. A. *Economic security of the enterprise. Textbook and workshop for universities.* Moscow, Yurayt Publ. House, 2019. 273 p. (In Russ.)

3. Khorev A. ., Sheremetov A. Yu., Barkalova I. I. Resource-functional approach as a method of ensuring the economic security of an enterprise. *Economics. Innovations. Quality management*, 2016, no. 4(17), pp. 76—78. (In Russ.)

4. Kovalenko T. V., Grinchenko E. V. Personnel security as an element of the economic security of an enterprise. *Innovation technologies in machine building, education and economics*, 2017, no. 3(5), pp. 19—22. (In Russ.)

5. *Federal Law "On Information, Information Technologies and Protection of Information" dated July 27, 2006 no. 149-FZ.* (In Russ.) URL: http://www.consultant.ru/document/cons_doc_LAW_61798.

6. *Federal Law "On Commercial Secret" dated July 29, 2004 no. 98-FZ.* (In Russ.) URL: http://www.consultant.ru/document/cons_doc_LAW_48699.

7. Split on bad terms. How the former employees complicate the companies' life. *RBC. Newspaper*, 2016, November 28 (no. 221). (In Russ.) URL: https://www.rbc.ru/newspaper/2016/11/29/582dbbb99a7947a46c6ca65b.

8. *15 surprises from dismissed employee: how employer can be prepared.* (In Russ.) URL: https://vc.ru/flood/14245-15-bad-employees.

9. Citizen of Komsomolsk-on-Amur is suspected in credit fraud. *Arguments and facts. Dalinform*, 2018, December 29. (In Russ.) URL: https://hab.aif.ru/incidents/komsomolchanku_podozrevayut_v_moshennichestve_na_kredite.

10. *STO BR IBBS-1.0-2014. Bank of Russia Standard "Ensuring the Information Security of Organizations of Banking System of the Russian Federation. General Provisions" (approved and put in force by the Bank of Russia Decree dated 17.05.2014 no. R-399).* (In Russ.) URL: https://cbr.ru/Content/Document/File/46921/st-10-14.pdf.

11. *Ernst & Young Global Limited Report Digital Signage Development.* (In Russ.) URL: https://www.ey.com/Publication/vwLUAssets/ey-digital-id-survey-rus/$FILE/ey-digital-id-survey-rus.pdf.

12. *Research on the level of information security in companies in Russia and the world for 2018.* (In Russ.) URL: https://searchinform.ru/uploads/sites/1/2019/03/research2018-searchinform.pdf.

13. *Dismissal of an employee leads to information leakage.* (In Russ.) URL: http://www.ukpz.com.ua/uvolnenie-sotrudnika-privodit-k-utechke-informacii.

14. *Investigation of information security incidents related to the actions of departing employees, 2018.* (In Russ.) URL: https://www.infowatch.ru/resources/analytics/reports/17083.

15. *What is personnel outplacement in Russia: types, steps and methods.* (In Russ.) URL: https://kakzarabativat.ru.

**Как цитировать статью**: Булатенко М. А., Тарасова Н. В. Применение технологии аутплейсмента для повышения уровня экономической безопасности предприятия // Бизнес. Образование. Право. 2020. № 4 (53). С. 128–135. DOI: 10.25683/VOLBI.2020.53.416.

**For citation**: Bulatenko M. A., Tarasova N. V. The use of outplacement technology to increase the level of economic security of the enterprise. *Business. Education. Law*, 2020, no. 4, pp. 128–135. DOI: 10.25683/VOLBI.2020.53.416.