УДК 338.242.2

ИНСАЙДЕРСКАЯ ДЕЯТЕЛЬНОСТЬ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В КОНЦЕПЦИИ КОНТРОЛЛИНГА

INSIDER ACTIVITY AS A THREAT TO ECONOMIC SECURITY IN THE CONTROLLING CONCEPT

[1]А.А. Пермовский, [2]В.П. Кузнецов

1. Нижегородский государственный педагогический университет им. К. Минина, Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1, email: ttpis@yandex.ru

Nizhny Novgorod State Pedagogical University named after. K. Minina, Russia, 603005, Nizhny Novgorod, st. Ulyanova, 1, email: ttpis@yandex.ru

2. Нижегородский государственный педагогический университет им. К. Минина, Россия, 603005, г. Нижний Новгород, ул. Ульянова, 1, email: kuzneczov-vp@mail.ru

Nizhny Novgorod State Pedagogical University named after. K. Minina, Russia, 603005, Nizhny Novgorod, st. Ulyanova, 1, email: kuzneczov-vp@mail.ru

Аннотация

В данной статье проанализированы такие понятия, как «инсайдер», «инсайдерская деятельность», «инсайдерская угроза». Рассмотрены задачи контроллинга экономической безопасности предприятия, причины разглашения инсайдерской информации. Обозначена актуальность инсайдерских угроз утечки информации для многих направлений бизнеса, присутствующих на рынке. Вопросы, рассматриваемые авторами в данной статье, в свете широкого применения и развития информационных технологий, количества несанкционированных воздействий на информационные системы и утечек инсайдерской информации, весьма актуальны. Авторами выделены основные виды сведений, которые чаще всего «утекают» из компаний, дана классификация видов внутренних нарушителей-инсайдеров. В данной статье обозначены основные и дополнительные направления для борьбы с инсайдерами. Данные меры должны способствовать формированию осознания неизбежности наказания за неправомерные действия и нанесенный ущерб предприятию. Задача многофункциональной системы контроллинга, в борьбе с угрозой экономической безопасности, заключается в систематизации и унификации операции.

Abstract

This article analyzes such concepts as "insider," "insider activity," "insider threat." The objectives of controlling the economic security of the enterprise, the reasons for the disclosure of insider information are considered. The relevance of insider threats of information leakage for many business areas present on the market is indicated. The issues considered by the authors in this article, in the light of the widespread use and development of information technologies, the number of unauthorized influences on information systems and leaks of insider information, are very relevant. The authors highlighted the main types of information that most often "leak" from companies, a classification of the types of internal insider violators is given. This article outlines the main and additional directions for dealing with insiders. These measures should contribute to the formation of an awareness of the inevitability of punishment for illegal actions and damage to the enterprise. The task of the multifunctional controlling system, in the fight against the threat to economic security, is to systematize and unify the operation.

Ключевые слова: экономическая безопасность, инсайдер, инсайдерская деятельность, контроллинг.

Keywords: economic security, insider, insider activity, controlling.

Введение. Развитие информационных технологий, хранение и обработка конфиденциальной информации в электронных базах данных, функционирующих в периметрах корпоративных сетей, создают угрозу утечек информации, которые могут произойти в результате умышленных действий пользователей информационных систем предприятий. Потенциально каждый сотрудник компании, а фактически это каждый легальный пользователь информационной системы предприятия, допущенный в соответствии со своими должностными обязанностями к информационным ресурсам, - потенциальный инсайдер. Поэтому борьба с инсайдерскими угрозами является важной задачей стратегического планирования при выявлении и минимизации рисков. Опираясь на идеологию и инструменты системы контроллинга, может решаться задача экономической безопасности предприятия.

Задачи контроллинга в контексте экономической безопасности компании могут включать:

– разработку инструментов и методов прогнозирования угроз экономической безопасности;

– оценку воздействия угроз на уровень экономической безопасности;

– обнаружение негативных тенденций развития событий при появлении угроз;

– создание методических рекомендаций по осуществлению комплекса мер для противостояния угрозам. [1]

В условиях цифровизации экономических систем возрастает потребность в разработке инструментов комплексного управления информацией. Данную потребность может обеспечить система контроллинга. Тем не менее, лишь небольшое число российских предприятий начинают применять функции данной системы. Эффективность контроллинга может служить смягчением против пагубного воздействия как внешних, так и внутренних обстоятельств на долгосрочную деятельность предприятия. Кроме того, внедрение контроллинга включает комплексный подход к развитию предприятия, учитывающий финансовые и экономические аспекты, использование функций превентивного управления.

Во многих компаниях модели контроллинга в основном ограничены задачами бухгалтерского учета, контроля и планирования, при этом мало внимания уделяется сохранности инсайдерской информации.

В своем первоначальном значении понятие «инсайдер» связывается с сотрудниками предприятия, имеющими доступ к корпоративной, непубличной или скрытой информации, способной повлиять на рыночную стоимость услуг, работ, товара предприятия и позволяющей получать выгоду при совершении сделок с ценными бумагами.

В таком же понимании инсайдерская деятельность рассматривается ст. 3.1.8 Инсайдерская торговля в Кодексе стандартов профессиональной этики. Согласно данной статье сотрудники не могут проводить сделки с ценными бумагами на основании инсайдерской информации, не имеют права использовать или обмениваться такой информацией для торговли ценными бумагами в личных целях.

Основная часть. Вместе с этим существующая действительность внесла коррективы в понятие инсайдера и расширила его границы.

В своих исследованиях Даниэль Коста определяет инсайдерскую угрозу как возможность человека, имеющего или имевшего ранее доступ к важным активам компании, злоупотреблять этим доступом намеренно или ненамеренно, что может негативно сказаться на организации [9].

Проводимые в настоящее время многочисленные исследования подтверждают актуальность инсайдерских угроз утечки информации для всех направлений бизнеса, присутствующих на рынке. При этом называются следующие виды сведений, которые чаще всего «утекают» из компаний: данные клиентов; детали конкретных сделок; финансовые отчеты; информация о топ-менеджменте компании. Информация может быть использована конкурентами для корректировки рыночной стратегии и привлечения клиентов, недобросовестными контрагентами компании для получения преимуществ. Все это может причинить ущерб компании, нанести удар по её репутации [6].

Таким образом, можно назвать ещё одно определение инсайдера – сотрудник компании, который в силу своего служебного положения имеет доступ к конфиденциальной информации и, нарушая установленные требования, разглашает информацию по своей халатности, либо использует или передает с целью получения личной выгоды.

Отметим основные причины:

– самым побуждающим к инсайдерской деятельности фактором назовем стремление получить материальное вознаграждение (корысть);

– на 2-м месте следует желание отомстить работодателю (возможно в контексте восстановления справедливости, защиты своих прав или личной неприязни), вызванное такими факторами как дисциплинарное взыскание, низкий уровень заработной платы, увольнение по инициативе работодателя;

– ещё одной частой причиной является халатность, небрежность и некомпетентность сотрудника. Например, работник мог нажать не ту кнопку (ошибка большого пальца) или перейти по ссылке на фишинговом сайте, подключить флеш-карту с вирусом;

– мотивация страхом, т.е. попытка запугать инсайдера с целью получения от него желаемой информации. Например, путем угроз жизни и здоровью его родным и близким.

Не касаясь подробного перечисления других мотивов инсайдеров, в целом можно всю их совокупность связать с одним понятием – лояльность работника к компании. Оценка лояльности работника является первоначальной мерой по снижению угроз от внутренних нарушителей. Разработка превентивных мер по противодействию инсайдерству на предприятии может быть одной из задач системы контроллинга. Кратко можно назвать следующие виды внутренних нарушителей-инсайдеров (Рисунок 1):

а) лояльные служащие, практически не нарушающие корпоративную политику безопасности. Они не нарушили внутренние правила безопасности, но их действия повлекли потерю информации (потенциальные угрозы: использование ненадежного пароля; неправильное включение/выключение оборудования; оставление без присмотра носителя информации и т.п.);

б) неумышленные нарушители, случайно нарушающие политику безопасности (потенциальные угрозы: переход по ссылке на фишинговом сайте с вирусом; удаление важной информации по халатности; пересылка информации по ошибочному адресу и т.п.);

в) нарушители, совершающие умышленные запрещенные действия (потенциальные угрозы: установка сторонних программ для передачи сообщений и информации; игнорирование установленных правил (стандартов) и т.п.);

г) нарушители «предатели», нынешние или бывшие служащие, внедренные инсайдеры передающие конфиденциальную информацию третьим лицам за вознаграждение или иным причинам.

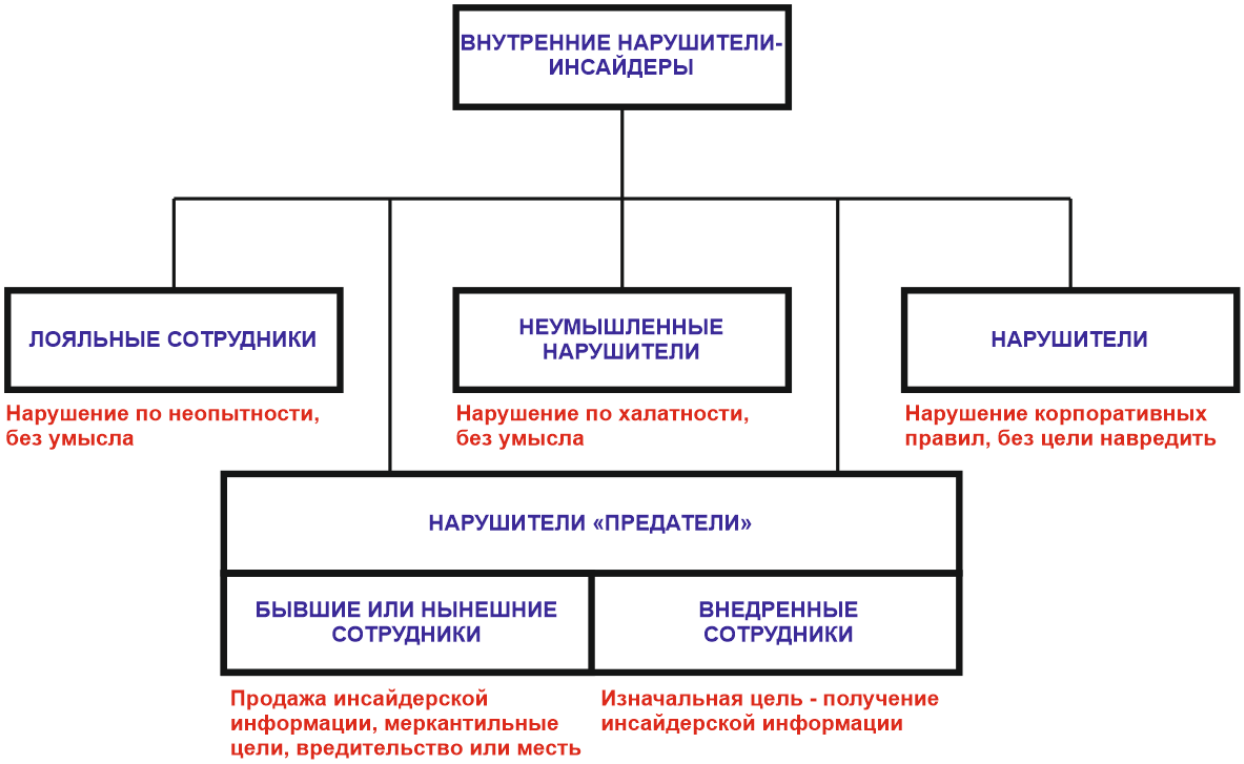

Рисунок 1. Виды внутренних нарушителей-инсайдеров
Источник: систематизировано по данным [7]

Также, в некоторых случаях, к внутренним нарушителям можно отнести партнеров, подрядчиков, временных сотрудников, привлеченных экспертов.

Как уже ранее отмечалось, одним из наиболее уязвимых звеньев в системе защиты является человек. Этот же фактор можно назвать и при рассмотрении мер борьбы с внутренними нарушителями. Нарушения могут отличаться по целям, мотивам, последовательности действий, но во всех случаях инсайдер не ломает систему, а использует предоставленные ему возможности.

Внедрение контроллинга включает комплексный подход к развитию предприятия, учитывающий использование расширенных функциональных возможностей и функций превентивного управления. Крайне важно, чтобы система контроллинга охватывала все аспекты деятельности предприятия. В этом контексте существует множество видов контроллинга, которые касаются либо процессов (маркетинг, производство, продажи и т.д.), либо ресурсов (финансовых, информационных и т.д.). Сегодня локализация контроллинга все чаще обосновывается в научных трудах. Однако доступ к этим процессам и ресурсам должен осуществляться комплексно (Рисунок 2).

Рисунок 2. Функциональная схема системы контроллинга
Источник: составлено автором

Для обеспечения безопасности компании необходимо разработать политику информационной безопасности – план, который обеспечит единство действий всей организации в вопросах предотвращения внутренних угроз и определения четких действий в случае их возникновения.

Необходимо включить в политику безопасности следующие области (Рисунок 3):

1. Соблюдение требований;
2. Защита инфраструктуры;
3. Восстановление данных;
4. Обучение сотрудников. [2]

Можно выделить следующие основные направления для борьбы с инсайдерами, которые могут предлагаться системой контроллинга на предприятиях:

– создание локальной нормативно-распорядительной базы на предприятии, регламентирующей порядок действий с конфиденциальной информацией, способов и мест ее хранения, меры ответственности за нарушения, включая обязательства о неразглашении коммерческой тайны;

– проверка принимаемых на работу сотрудников с целью выявления потенциальных нарушителей;

– ограничение доступа к инсайдерской информации;

– внедрение и развитие системы кибербезопасности;

– наличие системы контроля и управления доступом к различным информационным ресурсам предприятия, в том числе систем контроля и управления физическим доступом в помещения;

– внедрение и управление политикой безопасности в корпоративных сетях предприятий;

– осуществление мониторинга действий пользователей, проведение проверок по выявленным нарушениям;

– применение программно-технических средств, осуществляющих контроль использования каналов передачи данных;

– принятие мер воздействия к нарушителям;

– совершенствование системы управления. [5]

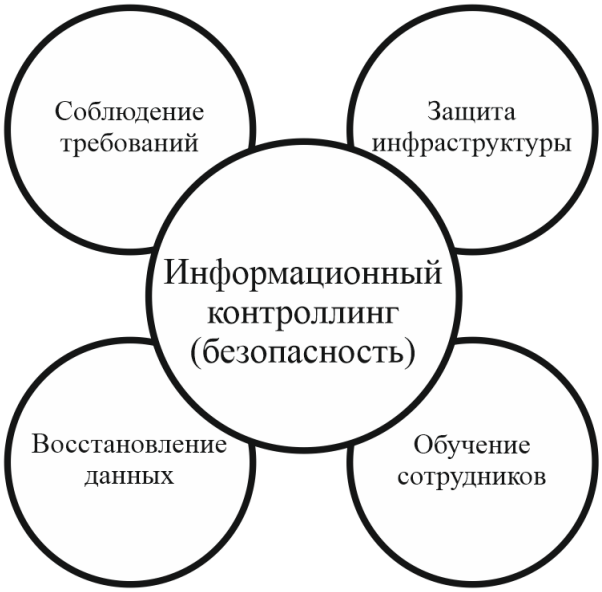

Рисунок 3. Области контроллинга информационной безопасности
Источник: систематизировано по данным [2]

Указанные меры реализуют комплексный подход. Следует особо выделить часть этих мер, а именно мониторинг действий пользователей, проверки по выявленным нарушениям, принятие мер воздействия к нарушителям направлены на формирование осознания неизбежности наказания за неправомерные действия и нанесенный ущерб.

Дополнительные меры для совершенствования системы борьбы с инсайдерскими утечками информации:

– доработка нормативных документов в области информационной безопасности, включение в них требования, что вся информация, созданная работником в рабочее время на оборудовании, принадлежащем компании, является собственностью компании. Данное требование основывается на положениях ФЗ «Об информации, информационных технологиях и о защите информации»;

– предварительная подготовка при увольнении сотрудников имеющих доступ к инсайдерской информации;

– контроль с помощью инновационных технических средств (к примеру, видеоконтроль с применением машинного зрения, «умные» браслеты-трекеры и т.п.).

Принимаемые меры должны анализироваться и сопоставляться с потенциальной угрозой.

Вывод. Повышенная опасность со стороны внутренних нарушителей требует рассматривать угрозы, связанные с внутренними сотрудниками, как одну из основных причин инцидентов в сфере информационной безопасности [8]. Реализация выше перечисленных мер должна способствовать формированию осознания неизбежности наказания за неправомерные действия и нанесенный ущерб. Эта задача на постоянной основе должна реализоваться системой контроллинга. Под руководством контроллера систематизируются и унифицируются операции, производимые сотрудниками внутренних подразделений предприятия, имеющих доступ к инсайдерской информации. Успешное развитие предприятия

может лишь при надлежащем обеспечении экономической безопасности [5]. Стабильность и безопасность компании, использующей контроллинг, значительно выше, чем у конкурентов [4]. Современный путь обеспечения экономической безопасности – адаптация к постоянным изменениям, автоматизация процессов технической защиты инсайда, минимизация человеческого фактора, применение технических инновационных средств защиты.

Список литературы

1. Ахмедов, Т. Ч. Неправомерное использование инсайдерской информации и манипулирование рынком в системе обеспечения экономической безопасности страны / Т. Ч. Ахмедов, А. Н. Литвиненко. – Санкт-Петербург : ООО "Издательство "ЛЕМА", 2023. – 172 с. – ISBN 978-5-00105-860-1.

2. Как застраховаться от утечек данных: план действий: РБК — URL: https://pro.rbc.ru/demo/66277e969a794798571008c8 (дата обращения: 28.04.2024).

3. Первова, Я. Э. Применение контроллинга в обеспечении экономической безопасности / Я. Э. Первова, М. В. Полубелова // Учет, анализ и аудит: проблемы теории и практики. – 2021. – № 26. – С. 125.

4. Романовская Е.В., Пермовский А.А., Бакулина Н.А., Скороходов И.С. Типы структур управления предприятием и их особенности // Московский экономический журнал. 2021. № 12. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-12-2021-70/ (дата обращения: 10.04.2024).

5. Романовская, Е. В. Взаимосвязь экологической и экономической безопасности предприятия: формы и оценка / С. Н. Кузнецова, Е. В. Романовская, Е. В. Конышкина [и др.] // Московский экономический журнал. – 2022. – Т. 7, № 4. – DOI 10.55186/2413046X_2022_7_4_206. – EDN JZEZQY.

6. Соломатова, Д. А. Понятие и содержание риск-контроллинга экономической безопасности на современном этапе / Д. А. Соломатова // Учет, анализ и аудит: проблемы теории и практики. – 2019. – № 22. – С. 212-219.

7. Тамбовская, Д. В. Инсайдерская деятельность в России: сущность и способы контроля / Д. В. Тамбовская, Н. И. Пшиканокова // Вестник Адыгейского государственного университета. Серия 5: Экономика. – 2018. – № 4(230). – С. 36-40. – EDN UFRBEL.

8. Шугаев, В. А. Классификация инсайдерских угроз информации / В. А. Шугаев, С. П. Алексеенко // Вестник Воронежского института МВД России. – 2020. – № 2. – С. 144.

9. CERT Определение «инсайдерской угрозы» — URL: https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/ (дата обращения: 14.04.2024).