МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра экономической теории
и национальной экономики

Информационный шпионаж и информационная безопасность предприятия

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 412 группы
Направления 38.03.01 «Экономика»
профиля «Экономика предприятий и организаций»
экономического факультета
Джуббаева Гуванча

Научный руководитель:
старший преподаватель _____ В. А. Максимов
должность, уч. степень, уч. звание подпись, дата инициалы, фамилия

Зав. кафедрой:
к.э.н., доцент _____ Е. В. Огурцова
должность, уч. степень, уч. звание подпись, дата инициалы, фамилия

Саратов 2026

Введение. Актуальность темы обусловлена тем, что в эпоху глобальной цифровизации информация трансформировалась в ключевой стратегический актив, определяющий конкурентные преимущества и рыночную стоимость предприятий. Информационный шпионаж перестал быть исключительной прерогативой государственных спецслужб, превратившись в распространённый инструмент недобросовестной конкуренции. Построение экономически обоснованной и эффективной системы информационной безопасности (ИБ) становится критически важным элементом стратегического управления, требующим не только технических, но и глубоких финансово-экономических обоснований.

Цель работы – проведение комплексного экономического анализа феномена информационного шпионажа и разработка экономически обоснованных рекомендаций по построению и совершенствованию систем информационной безопасности для минимизации связанных с ним финансовых рисков.

Задачи исследования:

1. Раскрыть экономическую сущность информационного шпионажа как формы недобросовестной конкуренции.
2. Определить экономическое содержание и стоимостные аспекты системы информационной безопасности предприятия.
3. Систематизировать современные методы выявления и предотвращения угроз ИБ, используемые на предприятиях.
4. Провести финансово-экономический анализ деятельности АО «УЭСК» и идентифицировать его критичные информационные активы, являющиеся потенциальными целями для шпионажа.
5. Проанализировать конкретный инцидент информационного шпионажа в АО «УЭСК» и оценить совокупный потенциальный экономический ущерб.
6. Рассчитать экономическую эффективность внедренных мер защиты и разработать рекомендации по совершенствованию системы ИБ.

Объект исследования – экономические отношения, возникающие в процессе противодействия информационному шпионажу в коммерческих организациях. Предмет – методы, инструменты и экономические последствия информационного шпионажа, а также экономические механизмы обеспечения ИБ (на примере АО «УЭСК»).

Методологическая основа – труды Абалкина Л.И., Сенчагова В.К., Гордона Л.А., Лоэба М.П., а также методы системного и сравнительного анализа, экономико-статистический метод, методы финансового и инвестиционного анализа.

Информационная база – нормативно-правовые акты РФ, бухгалтерская отчётность АО «УЭСК» за 2023–2025 гг., аналитические отчёты в сфере кибербезопасности, публикации в отраслевых СМИ.

Практическая значимость – разработанные подходы к оценке ущерба от киберинцидентов и расчёту экономической эффективности инвестиций в ИБ могут быть использованы руководителями коммерческих организаций для обоснования бюджетов на ИБ и интеграции управления киберрисками в общую систему риск-менеджмента.

Структура работы – введение, две главы, заключение, список использованных источников (40 наименований), приложения.

Основное содержание работы. В первой главе – «Теоретические основы информационного шпионажа и информационной безопасности в экономической сфере» – раскрыта экономическая сущность информационного шпионажа как формы недобросовестной конкуренции. В условиях цифровой экономики информация приобрела характеристики стратегического ресурса: невозвратность издержек на создание (затраты на НИОКР носят необратимый характер), минимальные предельные издержки тиражирования (стоимость копирования близка к нулю), синергетический эффект (ценность возрастает при комбинации с другими данными) и асимметричное распределение (обладание эксклюзивной информацией создаёт рыночную власть). Информационный шпионаж позволяет незаконно присваивать чужой информационный актив,

уклоняться от инвестиций в создание собственных знаний и перераспределять интеллектуальную ренту, что подрывает стимулы к инновациям и приводит к рыночной несостоятельности.

Представлена классификация информационного шпионажа по нескольким критериям. По субъекту (заказчик/исполнитель) выделяются: корпоративный (промышленный) шпионаж с прямым экономическим мотивом снижения издержек на НИОКР; заказной (от государства или криминала) с косвенным или прямым экономическим мотивом; внутренний (инсайдерский) – личный экономический мотив сотрудника. По объекту (типу информации) различаются: технологический шпионаж (направлен на присвоение результатов инновационной деятельности), коммерческий (клиентские базы, ценовые стратегии), управленческий/стратегический (долгосрочные намерения компании, планы M&A) и финансовый (конфиденциальные финансовые данные для манипуляции рынками). По масштабу потенциального экономического ущерба выделены катастрофический (угрожает существованию компании), существенный (серьёзно подрывает конкурентные позиции), умеренный (наносит поправимый ущерб) и незначительный (минимальные потери).

Разработана матрица экономических рисков информационного шпионажа, которая включает: риск потери доходов и доли рынка (прямые потери выручки, эрозия рыночной позиции), риск роста издержек (экстренные затраты на расследование и восстановление, рост постоянных издержек на безопасность), риск утраты инвестиций в НИОКР (амортизация затрат на разработки, снижение ожидаемой доходности будущих проектов), репутационный риск (падение доверия партнёров, снижение стоимости бренда), правовой и регуляторный риск (штрафы, судебные издержки), а также риск дезорганизации управления (утрата конкурентной стратегии, необходимость её срочного пересмотра).

Экономическое содержание системы информационной безопасности определено как комплекс управленческих и технологических механизмов, обеспечивающих сохранение экономической ценности информационных активов предприятия путём минимизации связанных с ними

рисков. Сформулированы ключевые принципы экономически обоснованной системы ИБ: принцип соразмерности затрат (инвестиции в защиту не должны превышать величину потенциального ущерба); принцип интеграции в систему управления стоимостью (защита должна быть встроена в ключевые бизнес-процессы); принцип непрерывного цикла управления рисками (идентификация активов → анализ угроз → оценка рисков в денежном выражении → выбор контрмер → мониторинг и переоценка); принцип измеримости через экономические показатели эффективности (ROSI, TCO, стоимость инцидента). Приведена классификация затрат на ИБ по виду (капитальные расходы CAPEX на создание инфраструктуры и операционные расходы OPEX на поддержание) и по цели (профилактические и на обнаружение/реагирование).

Систематизированы методы выявления и предотвращения угроз информационной безопасности. Экспертный метод основан на привлечении специалистов для качественной оценки рисков, его достоинства – низкие прямые затраты и учёт специфики бизнеса, недостатки – субъективность. Систематический (процессно-ориентированный) метод предполагает непрерывный мониторинг ИТ-инфраструктуры с помощью SIEM, IDS/IPS, управление уязвимостями и регулярные аудиты. Метод идентификации возможных источников угроз включает формализованное описание угроз по схеме «источник – уязвимости – способы реализации – объекты воздействия – последствия». Метод оценки вероятности реализации и ущерба переводит качественные угрозы в количественные показатели, позволяя ранжировать риски. Также выделены правовые методы (внутренние нормативные документы, соблюдение законодательства, NDA, меры ответственности), экономические методы (страхование киберрисков, создание резервов, система мотивации персонала) и технические методы (межсетевые экраны, антивирусы, DLP, EDR, NGFW). Комплексное применение всех групп методов обеспечивает многоуровневую защиту предприятия от информационного шпионажа.

Во второй главе – «Анализ информационного шпионажа и оценка экономической эффективности системы информационной безопасности АО «УЭСК»» – проведён практический анализ на примере реального предприятия.
Финансово-экономическая характеристика АО «УЭСК». Акционерное общество «Уральская энергетическая строительная компания» является ведущей строительной организацией в сфере энергетической инфраструктуры Уральского региона, осуществляет проектирование, строительство и реконструкцию линий электропередачи, подстанций и генерирующих мощностей. Основными заказчиками выступают крупные энергетические холдинги и государственные корпорации.

Горизонтальный анализ бухгалтерского баланса показал, что валюта баланса выросла на 42,6% в 2024 году (с 17,6 млрд руб. до 25,1 млрд руб.), однако в 2025 году снизилась на 16,6% (до 20,9 млрд руб.). Внеоборотные активы демонстрируют стабильный рост: в 2024 году – +105,7%, в 2025 году – +80,5%, что свидетельствует об активной инвестиционной фазе компании. Оборотные активы выросли на 38,4% в 2024 году, но снизились на 26,0% в 2025 году, в основном за счёт сокращения денежных средств (с 5 655 млн руб. до 1 820 млн руб., –67,8%) и дебиторской задолженности (с 15 941 млн руб. до 13 246 млн руб., –16,9%). Капитал и резервы растут опережающими темпами (+16,7% в 2024 году и +22,7% в 2025 году). Долгосрочные обязательства резко выросли в 2024 году (+204,9%) за счёт привлечения крупных инвестиционных кредитов. Краткосрочные обязательства выросли на 38,2% в 2024 году и снизились на 21,8% в 2025 году.

Вертикальный анализ актива баланса показывает, что доля внеоборотных активов выросла с 6,2% до 19,3% (+13,1 п.п.), а доля оборотных активов соответственно снизилась. Доля дебиторской задолженности выросла до 63,3% (+8,7 п.п. к 2023 году), что является очень высоким показателем и означает, что значительная часть активов находится в расчётах с контрагентами. Вертикальный анализ пассива баланса демонстрирует рост доли собственного капитала до 12,4% (+2,1 п.п.), рост доли долгосрочных обязательств (+5,7 п.п.) и

снижение доли краткосрочных обязательств (-7,8 п.п.), что свидетельствует о повышении долгосрочной финансовой устойчивости. Однако доля кредиторской задолженности остаётся высокой (69,2% в 2025 году).

Анализ отчёта о финансовых результатах показал устойчивый и ускоряющийся рост выручки: в 2024 году – +29,8%, в 2025 году – +48,5%. Валовая прибыль выросла на 70,0% в 2024 году (с 561 млн руб. до 953 млн руб.), но в 2025 году снизилась на 20,7% (до 756 млн руб.) из-за опережающего роста себестоимости (53,8% в 2025 году против 48,5% роста выручки). Прибыль от продаж выросла на 93,9% в 2024 году (рекордный показатель), но снизилась на 35,3% в 2025 году. Чистая прибыль растёт стабильными темпами: +14,0% в 2024 году и +15,8% в 2025 году, достигнув 480 млн руб. Рентабельность продаж по чистой прибыли снизилась с 3,5% до 2,4% (-1,1 п.п.), что свидетельствует о работе в условиях высокой конкуренции и сжатой маржи. Доля себестоимости в выручке выросла с 94,6% до 96,2% (+1,6 п.п.), что является негативным трендом.

Идентификация критичных информационных активов. На основе финансового анализа выделены наиболее ценные информационные активы АО «УЭСК», являющиеся потенциальными целями для информационного шпионажа (таблица 1).

Таблица 1 – Матрица критичности информационных активов АО «УЭСК»

№	Тип актива	Финансовый объем / характеристика	Потенциальная угроза	Критичность
1	Данные о дебиторской задолженности	13 245 млн руб. (63,3% активов)	Перехват платежей, инсайдерская торговля	Высокая
2	Тендерная и контрактная документация	Выручка 19 938 млн руб.	Передача конкурентам, срыв тендеров	Высокая
3	Финансовые вложения и инвестиционные планы	1 807 млн руб.	Получение инсайдерской информации	Высокая

Продолжение таблицы 1

4	ИТ-инфраструктура и системы управления	Обеспечение непрерывности	Блокировка (шифрование) всех данных	Критическая
5	Данные о кредиторах и расчетах	14 478 млн руб. кредиторской задолженности	Перенаправление платежей, фишинг	Высокая

Источник: Бухгалтерская (финансовая) отчетность АО «УЭСК» [Электронный ресурс]. – URL: https://bo.nalog.gov.ru/organizations-card/4264724 (дата обращения: 01.05.2026).

В июне 2025 года на информационную инфраструктуру АО «УЭСК» была совершена целенаправленная кибератака с использованием программ-шифровальщиков (ransomware). Согласно информации компаний «Софтлайн Решения» и Axoft, выступивших интеграторами по восстановлению и модернизации системы защиты, предприятие пережило инцидент с шифрованием данных. Особенностью атаки стало её комплексное воздействие: злоумышленники не только зашифровали критически важные данные, но и с высокой степенью вероятности осуществили их предварительное копирование с целью последующего вымогательства или продажи конкурентам. Инцидент классифицирован как внешняя криминальная атака с элементами технологического и коммерческого шпионажа.

Оценка потенциального экономического ущерба от инцидента (таблица 2) выполнена с учётом прямых потерь (восстановление данных, техническое расследование, усиление защиты, возможный выкуп, штрафы регуляторов) и косвенных потерь (простой бизнеса, утрата проектной документации, упущенная выгода от срыва тендеров, репутационный ущерб, рост стоимости кредитования).

Таблица 2 – Совокупная оценка потенциального ущерба, млн руб.

Категория потерь	Минимальная оценка	Максимальная оценка	Средняя оценка
Прямые потери	28,5	61	45

Продолжение таблицы 2

Косвенные потери	115	255	185
Совокупный ущерб (Y)	143,5	316	230

Источник: Составлено автором на основе проведенного анализа.

Совокупный потенциальный ущерб оценён в диапазоне от 143,5 до 316 млн рублей, при средней оценке около 230 млн рублей, что сопоставимо с половиной годовой чистой прибыли компании.

В ответ на инцидент компания внедрила комплекс мер, включающий межсетевой экран нового поколения (NGFW) с модулями IPS/IDS и обязательной аутентификацией, а также программный комплекс на базе SIEM (управление событиями и информацией безопасности) и EDR (обнаружение и реагирование на угрозы на конечных точках). Стоимость внедрения (CAPEX) составила 8,5 млн руб., ежегодные операционные расходы (OPEX) – 2,5 млн руб. Расчёт экономической эффективности выполнен на основе показателя возврата на инвестиции в безопасность (ROSI – Return on Security Investment). Годовые ожидаемые потери (ALE – Annual Loss Expectancy) до внедрения составляли 250 млн руб. × 0,6 = 150 млн руб., после внедрения – 250 млн руб. × 0,15 = 37,5 млн руб. Снижение годового риска – 112,5 млн руб. ROSI в первый год = (112,5 – 11,0) / 11,0 = 923%, что означает возврат 9,2 рубля предотвращённого ущерба на каждый вложенный рубль. Срок окупаемости капитальных затрат (8,5 млн руб.) составил менее 1 месяца. За три года эксплуатации системы совокупный чистый экономический эффект (предотвращённый ущерб за вычетом затрат) достигнет 321,5 млн руб.

Внедрённая система полностью соответствует принципам экономически обоснованной информационной безопасности: затраты многократно меньше величины предотвращённого ущерба (11 млн руб. против 250 млн руб. стоимости инцидента), обеспечена интеграция с существующей ИТ-инфраструктурой, сбалансированы капитальные и операционные расходы.

Разработка рекомендаций по совершенствованию системы информационной безопасности. На основе проведённого анализа и лучших отраслевых практик предложен комплекс дополнительных мероприятий (таблица 3).

Таблица 3 – Сводная таблица рекомендуемых мероприятий и их экономическая оценка

Мероприятие	CAPEX, млн руб.	OPEX, млн руб./год	Ожидаемый экономический эффект	Рекомендуемый приоритет
Страхование киберрисков	–	3–5	Передача рисков, прямая компенсация ущерба до 100 млн руб.	Высокий
Финансовый резерв на реагирование	30–40	–	Снижение времени простоя, оперативность реагирования	Высокий
Пентесты (1 раз в год)	0,5–1,5	–	Выявление «слепых зон»; предотвращение критических уязвимостей	Средний
Обучение персонала (антифишинг)	–	1–2	Снижение риска социальной инженерии на 70–80%	Высокий
Внедрение DLP	3–5	1–2	Предотвращение утечки проектной документации (ущерб 30–100 млн руб.)	Средний
Аутсорсинг SOC / MDR	–	5–10	Снижение ущерба от невыявленных угроз на 30–50%	Средний

Источник: Составлено автором на основе проведенного анализа.

Реализация рекомендуемых мероприятий позволит дополнительно снизить риски информационного шпионажа, обеспечить круглосуточный мониторинг, повысить осведомлённость персонала и создать финансовую «подушку безопасности» для оперативного реагирования на инциденты.

Заключение. Проведённое в рамках выпускной квалификационной работы исследование позволяет сформулировать следующие основные выводы.

По теоретической части: информационный шпионаж представляет собой форму недобросовестной конкуренции, направленную на незаконное присвоение чужого информационного ресурса, что подрывает стимулы к инновациям, искажает рыночные механизмы и создаёт системные экономические риски. Экономическое содержание системы информационной безопасности определяется как сохранение экономической ценности информационных активов путём управления рисками. Ключевые принципы экономически обоснованной ИБ – соразмерность затрат, интеграция в управление стоимостью, непрерывность цикла управления рисками и измеримость через экономические показатели (ROSI, TCO, стоимость инцидента). Методы выявления и предотвращения угроз включают экспертные, систематические, правовые, экономические и технические подходы, эффективность которых достигается только при комплексном применении.

По практической части: АО «УЭСК» является крупной строительной компанией с устойчивым ростом выручки (+92,8% за три года) и чистой прибыли (+32,2%). Однако структура активов характеризуется высокой долей дебиторской задолженности (63,3% активов) и кредиторской задолженности (69,2% пассивов), что делает критически важной защиту систем ДБО и конфиденциальности расчётов. Ключевыми информационными активами, подлежащими приоритетной защите, являются данные о дебиторской и кредиторской задолженности, тендерная документация, финансовые вложения и ИТ-инфраструктура.

Произошедший инцидент информационного шпионажа (атака с шифрованием данных) подтвердил реальность угрозы; совокупный потенциальный экономический ущерб оценён в диапазоне 143,5–316 млн руб. (средняя оценка – 230 млн руб.), что сопоставимо с половиной годовой чистой прибыли. Внедрённый комплекс мер (NGFW + SIEM + EDR) обеспечил ROSI на уровне 923% (каждый рубль инвестиций приносит 9,2 рубля предотвращённого

ущерба) и срок окупаемости менее 1 месяца, что доказывает сверхвысокую экономическую эффективность инвестиций в проактивную комплексную информационную безопасность.

Разработанные дополнительные рекомендации (страхование киберрисков, создание финансового резерва, регулярные пентесты, обучение персонала, внедрение DLP, аутсорсинг SOC) позволят усилить защиту с учётом эволюции угроз и изменений в бизнес-среде, обеспечив дальнейшее снижение рисков и сохранение стоимости бизнеса.

Таким образом, цель работы достигнута. Результаты исследования могут быть использованы руководителями коммерческих организаций, специалистами служб экономической и информационной безопасности для обоснования бюджетов на создание и модернизацию систем защиты информации, а также в учебном процессе при преподавании дисциплин, связанных с экономической безопасностью и управлением рисками.