МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА,
ЭКОНОМИКИ И УПРАВЛЕНИЯ

КАФЕДРА ЭКОНОМИКИ И УПРАВЛЕНИЯ

ОТЧЕТ
по учебной практике по получению навыков исследовательской работы

ООО «Компания «Верфь-Бизнес», г. Владивосток

Студент
группы ВДБЭУ-24-ФЭ1 _____ А.К. Кузьменко

Руководитель
канд. экон. наук, доцент _____ А.А. Вертинова

Нормоконтролер
канд. экон. наук, доцент _____ А.А. Вертинова

Владивосток 2025

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВВГУ»)
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ

КАФЕДРА ЭКОНОМИКИ И УПРАВЛЕНИЯ

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на учебную практику по получению навыков исследовательской работы

Студент: Кузьменко Алина Константиновна
Группа: ВДБЭУ-24-ФЭ1
Срок сдачи: 19.04.2025

Содержание отчета по учебной практике по получению навыков исследовательской работы:

Введение: определить цель и задачи практики, основные методы, необходимые для их достижения (Объем – 1 страница)

Раздел 1. Характеристика исследуемой проблемы по теме «Информационная безопасность в цифровой экономике»

Краткое содержание исследуемой проблемы и ее актуальность, степень разработанности исследуемой проблемы (перечень авторов, внесших вклад в решение проблемы; отражение проблемы в государственных нормативных документах и т.п.); цель и задачи исследования (УК-1.1в, УК-1.3в).

Раздел 2. Современное состояние исследуемой проблемы

Сущность исследуемой проблемы в авторском изложении с иллюстрацией, статистическим и аналитическим материалом, перспективы дальнейших исследований по данной теме (УК-1.1в). (Объем двух разделов – 10-12 страниц)

Заключение. В заключении обобщается изложенный в отчете материал, делаются выводы. (Объем – 1-2 страницы)

Список использованных источников (включаются источники не старше 5 лет от даты использования).

Руководители практики
канд. экон. наук, доцент кафедры ЭУ _____ А.А. Вертинова
Задание получил: _____ Кузьменко А. К.

РАБОЧИЙ ГРАФИК (ПЛАН)
ПРОВЕДЕНИЯ УЧЕБНОЙ ПРАКТИКИ ПО ПОЛУЧНИЮ НАВЫКОВ ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Студент _____Кузьменко Алина Константиновна_____
_____
Фамилия Имя Отчество

Кафедра экономики и управления гр._____ВДБЭУ-24-ФЭ1_____

Руководители практики_____Вертинова Анна Александровна_____
Фамилия Имя Отчество

Инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности прошел
_____
(подпись уполномоченного лица, МП)

С правилами трудового распорядка ознакомлен_____ Кузьменко А. К.
(подпись обучающегося)

Этапы практики	Виды работы	Срок выполнения	Отметка руководителя о выполнении
1. Подготовительный	Организационное собрание	1.04.2025	
2. Исследовательский	Формулировка целей и задач исследования	7.04.2025	
3. Аналитический	Подбор и анализ информации по теме исследования	15.04.2025	
4. Заключительный	Подготовка и защита отчета	19.04.2025	

Руководители практики

канд. экон. наук,
доцент кафедры ЭУ _____ А.А. Вертинова

Содержание

Введение

Цифровая трансформация экономики оказывает существенное влияние на все сферы современного общества, формируя новые подходы к организации производственных процессов, управлению данными, коммуникации и принятию решений. В этих условиях информационные технологии становятся не только инструментом развития, но и источником новых рисков и угроз. Одной из ключевых проблем, сдерживающих развитие цифровой экономики, является обеспечение информационной безопасности — состояния защищённости информации и инфраструктур от внутреннего и внешнего несанкционированного воздействия, способного нанести ущерб интересам личности, общества и государства.

Информационная безопасность (ИБ) в цифровой экономике — это комплексная проблема, охватывающая технические, организационные, правовые и социальные аспекты. Повышение числа инцидентов, связанных с утечками данных, хакерскими атаками, кибермошенничеством, распространением вредоносного ПО, свидетельствует о росте уязвимостей в цифровой среде. В частности, по данным отчёта «Positive Technologies» за 2023 год, количество утечек конфиденциальной информации увеличилось на 18 % по сравнению с предыдущим годом, при этом 65 % инцидентов были связаны с человеческим фактором и недостатками в управлении ИБ.

В условиях цифровой трансформации возрастает значение правового регулирования и создания эффективной системы управления информационной безопасностью. В России эти вопросы регулируются рядом нормативных документов, включая Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также указами Президента РФ и Стратегией развития информационного общества на 2017–2030 годы. Также активно развиваются международные подходы, включая стандарты ISO/IEC серии 27000.

Учитывая важность рассматриваемой темы, учебная практика была направлена на формирование у обучающегося первичных исследовательских навыков, способствующих осмыслению проблем ИБ и разработке предложений по их решению.

Цель учебной практики — формирование практических умений анализа проблем информационной безопасности в цифровой экономике, овладение методами исследования и интерпретации научных и нормативных данных, а также развитие навыков самостоятельной исследовательской работы.

Для достижения поставленной цели были сформулированы следующие задачи:

1. Изучить научную литературу и нормативно-правовые акты в области информационной безопасности и цифровой экономики;
2. Проанализировать основные угрозы и уязвимости, возникающие в условиях цифровизации;
3. Ознакомиться с методами оценки рисков и построения систем защиты информации;
4. Проанализировать отечественные и международные подходы к обеспечению ИБ в цифровой среде;
5. Выработать предложения по повышению уровня защищённости информационных ресурсов в цифровой экономике.

В рамках практики использовались следующие методы исследования:

- Анализ нормативных документов — для выявления структуры регулирования в области ИБ;
- Контент-анализ научных публикаций — для определения ключевых направлений исследований;
- Сравнительный анализ — при изучении зарубежного и российского опыта в обеспечении ИБ;

- Системный подход — для комплексного осмысления проблемы и выстраивания логической структуры угроз и методов их предотвращения;
- Анализ статистических данных — для подтверждения актуальности проблематики на основе реальных кейсов и инцидентов.

Актуальность данной темы определяется не только научным и практическим значением проблемы, но и необходимостью развития новых компетенций у специалистов, способных разрабатывать и реализовывать эффективные стратегии обеспечения ИБ в рамках цифровой экономики. Современные вызовы требуют от исследователей и практиков гибкого подхода к анализу угроз, прогнозированию рисков и созданию адаптивных систем защиты информации.

Содержание и результаты учебной практики направлены на углубление профессиональных знаний в области информационной безопасности, развитие исследовательских навыков, а также формирование системного понимания актуальных проблем цифровой экономики в контексте информационной защищённости.

1 Характеристика исследуемой проблемы по теме «Информационная безопасность в цифровой экономике»

1.1 Актуальность и содержание исследуемой проблемы

В условиях стремительного развития цифровой экономики информационные технологии становятся ключевым элементом экономической и социальной инфраструктуры. Электронные платформы, облачные сервисы, распределённые вычисления, интернет вещей (IoT), системы искусственного интеллекта и большие данные (Big Data) внедряются во все сферы: от государственного управления и здравоохранения до банковского сектора и розничной торговли. Однако, наряду с несомненными преимуществами, цифровизация порождает и серьёзные вызовы, прежде всего в области информационной безопасности (ИБ).

Информационная безопасность в цифровой экономике — это не просто защита информации от несанкционированного доступа или разрушения, а ключевой фактор устойчивости цифровой среды. От уровня защищённости информационных систем напрямую зависит работоспособность бизнес-процессов, сохранность персональных данных граждан, доверие к цифровым сервисам и национальная безопасность в целом [1].

Цифровая экономика не может эффективно развиваться без доверия участников к защищённости инфраструктуры. ИБ становится фактором инвестиционной привлекательности, основой функционирования цифрового правительства, электронных рынков, цифровых финансов и платформенной модели взаимодействия бизнеса и государства [2]. В этой связи государственные стратегии, такие как Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, подчёркивают необходимость формирования эффективной системы обеспечения информационной безопасности в условиях цифровой трансформации [3].

Кроме того, ИБ рассматривается как важный элемент цифрового суверенитета страны. В условиях нарастающего киберпротивостояния между

государствами вопросы защиты информации и управления цифровыми рисками приобретают стратегическое значение [4].

С развитием цифровых технологий расширяется и спектр угроз информационной безопасности. Эти угрозы можно условно разделить на внутренние и внешние. К внешним угрозам относятся кибератаки, вирусные программы, фишинг, DDoS-атаки, кибершпионаж, целевые атаки на критически важную информационную инфраструктуру. Внутренние угрозы чаще всего связаны с нарушениями регламентов, действиями сотрудников, несанкционированным доступом и утечками данных по неосторожности или злому умыслу [5].

По данным Positive Technologies, в 2023 году зафиксировано более 2000 инцидентов, связанных с утечками персональных и конфиденциальных данных, из которых около 65 % были вызваны внутренними факторами — ошибками пользователей, отсутствием контроля доступа и слабой политикой аутентификации [6]. Одновременно наблюдается рост количества и сложности целенаправленных атак с применением методов социальной инженерии и вредоносного ПО.

В условиях цифровизации особую угрозу представляют уязвимости в программном обеспечении, сбои в системах киберзащиты, а также недостаточный уровень готовности организаций к реагированию на инциденты. Как отмечают Шабанов А.В. и Орлова М.Н., несмотря на активное развитие ИТ-инфраструктуры, уровень зрелости систем ИБ в большинстве организаций остаётся недостаточным [5].

К числу глобальных вызовов также относится зависимость от зарубежных цифровых платформ и сервисов, что особенно актуализировалось в условиях санкционного давления. Уязвимость поставок программного обеспечения, ограничение доступа к международным ИТ-решениям и нарушение логистики цифровых технологий усиливают необходимость

развития национальных систем и стандартов информационной безопасности [4].

Таким образом, в цифровой экономике формируется комплексная угроза, охватывающая технические, организационные, правовые и человеческие аспекты. Это требует системного подхода к формированию архитектуры информационной безопасности, охватывающей весь жизненный цикл цифровых решений: от проектирования до эксплуатации и утилизации.

Информационная безопасность напрямую влияет на устойчивое функционирование цифровой инфраструктуры, включая государственные платформы, финансовые системы, энергетические и транспортные сети. Любой серьёзный инцидент ИБ может привести к остановке бизнес-процессов, финансовым потерям, утрате доверия потребителей и партнёров, а в случае критической инфраструктуры — к социальным и экономическим катастрофам [7].

В современных условиях устойчивость цифровой инфраструктуры невозможно представить без интеграции механизмов обеспечения ИБ на всех уровнях — технологическом, организационном и нормативном. Как подчёркивают Колосов Д.Ю. и Лебедев С.В., информационная безопасность становится не просто элементом защиты, а стратегическим инструментом управления рисками и обеспечения деловой непрерывности [7; 8].

Кроме того, высокий уровень ИБ способствует повышению инвестиционной привлекательности компаний и стран в целом, так как защищённая цифровая среда способствует развитию новых цифровых сервисов и инновационных бизнес-моделей [2]. Без эффективной защиты информации невозможно внедрение облачных технологий, блокчейн-решений, систем искусственного интеллекта, поскольку именно доверие к технологической платформе определяет готовность пользователей к её использованию.

На государственном уровне важную роль играет развитие системы управления безопасностью критической информационной инфраструктуры. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» закрепляет комплекс организационных и технологических мер по защите объектов, имеющих ключевое значение для устойчивости экономики и безопасности государства [9].

Обеспечение информационной безопасности — это необходимое условие для долгосрочного и устойчивого развития цифровой экономики, цифрового государства и общества. Без надёжной защиты информации невозможно формирование цифрового пространства, в котором соблюдаются права граждан, сохраняется цифровой суверенитет, а бизнес развивается в безопасной и предсказуемой среде [3; 10].

1.2 Степень разработанности проблемы

Информационная безопасность как научная и прикладная дисциплина начала формироваться в России и за рубежом с конца XX века, а в условиях стремительной цифровизации её значение значительно возросло. Сегодня данное направление является предметом междисциплинарного исследования, включающего аспекты информатики, права, экономики, социологии и управления.

Среди отечественных авторов, внёсших значительный вклад в разработку теоретических основ информационной безопасности, можно выделить И.А. Васильева, который акцентирует внимание на роли ИБ в цифровой экономике, её взаимосвязи с инновационным развитием и необходимостью перехода от концепции защиты информации к концепции устойчивого цифрового развития [1]. Его работы подчёркивают необходимость системного подхода к обеспечению ИБ на всех уровнях: от отдельных информационных систем до государственной политики.

Другой важный автор — А.В. Шабанов, который вместе с М.Н. Орловой классифицирует современные угрозы в условиях цифровизации и выделяет уязвимости, присущие платформенной модели экономики [5]. По мнению авторов, большинство существующих систем ИБ не способны эффективно реагировать на гибридные угрозы, сочетающие технические и социальные воздействия. Шабанов акцентирует внимание на недостаточном уровне защищённости российских организаций и предлагает адаптивные модели ИБ, основанные на анализе рисков и машинном обучении.

В числе зарубежных исследователей важнейшее место занимает Брюс Шнайер — признанный эксперт в области криптографии, кибербезопасности и цифровой политики. В своей работе Click Here to Kill Everybody он подчёркивает, что в эпоху гиперсвязанности любая цифровая уязвимость может иметь физические последствия, особенно в контексте критической инфраструктуры [11]. Шнайер рассматривает ИБ как общественное благо, которое требует государственного регулирования и международной кооперации.

Значительный вклад также внесён авторами, работающими в рамках международных стандартов ISO/IEC. Их подход основывается на создании систем управления информационной безопасностью (ISMS), ориентированных на оценку рисков, внедрение политик безопасности и постоянное улучшение механизмов защиты [12].

Таким образом, как отечественная, так и международная научная мысль в области ИБ развивается в направлении системного, риск-ориентированного и процессного подходов, отражая комплексную природу исследуемой проблемы.

Современные концепции информационной безопасности опираются на принцип многоуровневой защиты, предполагающей применение технических, организационных и правовых мер. Основными элементами таких моделей

являются: защита периметра, контроль доступа, мониторинг событий, аудит, реагирование на инциденты и восстановление после атак.

Одной из самых известных и применяемых моделей является модель CIA (Confidentiality, Integrity, Availability) — конфиденциальность, целостность и доступность. Эти три принципа лежат в основе международных стандартов безопасности информации, включая ISO/IEC 27001 [12]. На практике модель CIA дополняется принципами аутентичности, ответственности, надёжности и отказоустойчивости.

Наиболее прогрессивной моделью последних лет считается Zero Trust Architecture (архитектура нулевого доверия), основанная на предпосылке, что никакая система или пользователь не должен автоматически считаться доверенным — даже если он находится внутри периметра организации. Этот подход активно внедряется в ведущих мировых ИТ-компаниях и получает поддержку на уровне государственных структур.

В России также применяются подходы, основанные на ГОСТ Р 57580.1-2017 и национальных методиках оценки рисков ИБ, рекомендованных Федеральной службой по техническому и экспортному контролю (ФСТЭК). При этом государственное регулирование всё чаще нацелено на интеграцию ИБ в общую стратегию цифровой трансформации, что отражено, в частности, в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [3].

Ключевым понятием становится информационная устойчивость (resilience) — способность системы функционировать в условиях атаки, быстро восстанавливаться и адаптироваться к новым угрозам. В рамках этой парадигмы важную роль играют предиктивные технологии, анализ больших данных и искусственный интеллект [2].

Однако, несмотря на существование множества концепций, на практике их реализация в организациях остаётся неполной. По данным отчёта Positive Technologies за 2023 год, только 38 % компаний в России применяют

комплексный подход к управлению ИБ, тогда как большинство организаций ограничиваются базовыми средствами защиты [6].

Таким образом, в существующих моделях ИБ наблюдается переход от фрагментарного подхода к целостной архитектуре, интегрированной в корпоративное и государственное управление, однако уровень их внедрения пока остаётся неоднородным.

Развитие информационной безопасности невозможно без активного участия профессионального сообщества, объединяющего экспертов, практиков, научных работников, разработчиков и представителей регуляторов. Сегодня в России и за её пределами действуют десятки организаций и платформ, способствующих обмену знаниями, разработке стандартов и продвижению лучших практик в области ИБ.

Одной из ведущих российских платформ является Ассоциация специалистов по информационной безопасности (АСИБ), которая проводит научные конференции, издаёт журнал Информационная безопасность, участвует в разработке ГОСТов и методических рекомендаций. Значимую роль играет ФСТЭК России, как главный регулятор в области защиты информации, а также ЦБ РФ, который активно развивает стандарты ИБ в финансовом секторе.

Ведущие исследовательские центры и лаборатории, такие как Group-IB, Kaspersky Lab, Positive Technologies, не только разрабатывают собственные решения, но и публикуют ежегодные аналитические отчёты об угрозах, тенденциях и уязвимостях. Так, Threat Intelligence Report 2023 от Group-IB предоставляет детальный анализ киберугроз по отраслям и странам [13], а отчёт Positive Technologies за 2023 год выделяет основные сценарии атак и типовые ошибки в корпоративных системах [6].

На международном уровне ведущими центрами являются SANS Institute, ENISA (Агентство Европейского союза по кибербезопасности), а также исследовательские лаборатории при университетах — MIT, Stanford,

Cambridge. Эти структуры формируют глобальные повестки, участвуют в стандартизации и продвигают новые научные идеи.

Особую роль в развитии научной мысли играют международные и всероссийские конференции по ИБ, где обсуждаются вызовы цифровой трансформации, безопасность критической инфраструктуры, киберустойчивость и защита данных. Участие в них позволяет синхронизировать усилия научного сообщества, практиков и власти.

Кроме того, в последние годы важной тенденцией стало создание отраслевых центров мониторинга и реагирования на инциденты ИБ (SOC). Эти центры аккумулируют информацию о текущих угрозах, моделируют атаки и формируют базы знаний, доступные для участников профессионального сообщества.

Взаимодействие научных, государственных и коммерческих организаций играет ключевую роль в развитии сферы ИБ, особенно в условиях стремительного технологического прогресса и постоянного появления новых угроз. Профессиональное сообщество не только формирует повестку, но и определяет направления нормативного, методического и практического развития информационной безопасности.

1.3 Нормативно-правовое регулирование и цель исследования

Нормативно-правовая база является основой обеспечения информационной безопасности в цифровой экономике. В Российской Федерации система регулирования в данной сфере охватывает широкий круг нормативных актов федерального и подзаконного уровня, а также учитывает международные стандарты и рекомендации.

Ключевым документом, регулирующим обращение с информацией и информационными технологиями, является Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [14]. Данный закон определяет основные понятия,

принципы обеспечения безопасности информации, а также устанавливает правовой режим для защиты как государственной, так и персональной информации. Особое внимание уделяется защите информации, составляющей государственную тайну, персональных данных, коммерческой и служебной тайны.

Немаловажное значение имеет Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [9]. Он направлен на защиту объектов критической ИТ-инфраструктуры — таких как системы управления транспортом, энергетикой, банковскими структурами и здравоохранением — от киберугроз и внешнего воздействия. Закон регулирует порядок категорирования объектов КИИ, обязанности операторов КИИ и ответственность за нарушения режима ИБ.

Особое место среди стратегических документов занимает Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утверждённая Указом Президента РФ от 9 мая 2017 года № 203 [3]. В разделе IV данной стратегии подчёркивается, что создание эффективной системы информационной безопасности является неотъемлемым условием развития цифровой экономики. Стратегия предусматривает формирование системы управления рисками, развитие кадрового потенциала и совершенствование механизмов государственной защиты информации.

На международном уровне важнейшую роль играют стандарты ISO/IEC, в частности:

- ISO/IEC 27001:2022 — стандарт, определяющий требования к системам управления информационной безопасностью (ISMS) [12];
- ISO/IEC 27002 — рекомендации по мерам безопасности;
- ISO/IEC 27701 — стандарт по защите персональных данных и расширение к ISO 27001.

Эти документы используются в качестве ориентиров для разработки внутренних политик ИБ в организациях, а также при сертификации систем защиты. Международные стандарты применимы не только в частных, но и в государственных структурах, поскольку обеспечивают универсальность подходов и сопоставимость с глобальной практикой.

Нормативно-правовая база в сфере информационной безопасности формируется на основе сочетания национальных законов и международных стандартов, обеспечивая комплексный и многоуровневый подход к решению задач защиты информации в условиях цифровой экономики.

Цель учебной практики по теме «Информационная безопасность в цифровой экономике» заключается в формировании практических и аналитических навыков, необходимых для комплексного осмысления проблематики ИБ, анализа нормативных актов, научной литературы, статистических данных и предложений по повышению уровня защищённости цифровой среды.

В рамках учебной практики ставятся следующие задачи:

1. Изучить и систематизировать ключевые понятия, принципы и цели информационной безопасности в цифровой экономике;
2. Ознакомиться с действующей нормативно-правовой базой Российской Федерации и международными стандартами, регулирующими сферу ИБ;
3. Проанализировать научные подходы к классификации угроз, моделей защиты информации и методов реагирования на киберинциденты;
4. Исследовать современные угрозы и тенденции развития цифровых рисков;
5. Ознакомиться с примерами реализации систем ИБ в различных отраслях (на основе открытых кейсов и аналитических данных);
6. Выявить ключевые проблемы и «узкие места» в организации ИБ на уровне предприятий и государства;

7. Сформулировать предложения и рекомендации по совершенствованию системы обеспечения ИБ в цифровой экономике.

Практика предполагает работу как с теоретическим, так и прикладным материалом — от чтения законодательства и аналитических отчётов (например, Positive Technologies, Group-IB [6; 13]) до изучения конкретных примеров реализации программ ИБ в корпоративной и государственной сферах. Итогом исследования становится структурированный отчёт, содержащий аналитические выводы и предложения, подготовленный в соответствии с академическими стандартами.

В процессе прохождения учебной практики и выполнения исследовательской работы по теме информационной безопасности в цифровой экономике формируются и развиваются следующие универсальные компетенции, предусмотренные образовательными стандартами высшего образования:

УК-1.1в.

Способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения задач.

В рамках практики обучающийся учится работать с различными источниками информации — законодательными актами, научными публикациями, аналитическими отчётами, статистикой, — оценивая их достоверность и значимость. Он применяет логико-структурные схемы для анализа угроз, моделей и факторов риска. Это позволяет глубже понять сущность проблем, выработать обоснованные выводы и предложить реалистичные решения.

УК-1.3в.

Способность использовать основы системного и критического мышления в профессиональной деятельности, включая междисциплинарные задачи.

Исследование в области ИБ требует сочетания знаний из различных дисциплин: информационных технологий, права, управления, экономики. В ходе практики формируется умение оценивать явления с различных точек зрения, анализировать взаимосвязи между элементами системы ИБ, принимать решения с учётом множества факторов (технических, правовых, социальных и др.).

Дополнительно в процессе работы развиваются и другие метакомпетенции:

- коммуникативная компетентность — при оформлении и представлении результатов исследования;
- аналитическая компетентность — при интерпретации количественных и качественных данных;
- информационная грамотность — при поиске и верификации цифровых источников.

Учебная практика не только способствует углублению знаний по теме, но и обеспечивает подготовку к реальной профессиональной деятельности в условиях цифровой трансформации экономики и растущих требований к специалистам в сфере информационной безопасности.

2 Современное состояние исследуемой проблемы

2.1 Анализ текущей ситуации в области информационной безопасности

Современная цифровая экономика развивается в условиях постоянного роста киберугроз и усложнения атакующих технологий. В последние пять лет количество инцидентов информационной безопасности в России и в мире увеличивается ежегодно. Особую озабоченность вызывают атаки на критическую информационную инфраструктуру, массовые утечки персональных данных и применение программ-вымогателей.

В таблице 1 представлена динамика зарегистрированных киберинцидентов в Российской Федерации за последние пять лет. Данные получены на основе открытых аналитических отчётов компаний Positive Technologies, Group-IB и мониторинга RED Security SOC.

Таблица 2.1 – Количество киберинцидентов в РФ (2020–2024 гг.)

Год	Количество инцидентов (тыс.)	Рост по сравнению с предыдущим годом (%)
2020	1,2	–
2021	1,5	25,0
2022	1,9	26,7
2023	2,2	15,8
2024	2,5	13,6

По оценке специалистов RED Security SOC, в 2024 году количество атак выросло в 2,5 раза по сравнению с 2023 годом, если учитывать только целевые инциденты с высокой критичностью. Особенно активно атакуются объекты критической инфраструктуры — на них приходится более 64 % всех атак [15].

Одной из главных тенденций остаётся рост атак с использованием программ-вымогателей (ransomware), доля которых увеличилась на 44 % по

сравнению с предыдущим годом. Параллельно фиксируется увеличение фишинговых рассылок — они составляют до 69 % всех киберугроз [6].

Современные ИТ-системы подвержены целому ряду уязвимостей, как технического, так и организационного характера. Основные слабые места систем ИБ представлены в таблице 2, в сравнении между 2020 и 2024 годами.

Таблица 2.2 – Типы киберугроз и их распространённость (% от общего числа атак)

Тип угрозы	2020 (%)	2024 (%)
Фишинг	25	38
Программы-вымогатели	18	35
Вредоносное ПО	20	16
Эксплойты	15	13
Инсайдерские действия	7	10

Из таблицы видно, что особенно активно растёт доля фишинга и программ-вымогателей. В 2024 году на открытых ресурсах было выявлено более 259 ранее не публиковавшихся баз данных с персональными данными российских граждан, попавших в открытый доступ [источник: rbc.ru, 2024].

Кроме технических уязвимостей, опасность представляют организационные факторы: устаревшее ПО, слабая защита облачных решений, незащищённые IoT-устройства и отсутствие сегментации сетей.

Несмотря на развитие технологий, человеческий фактор остаётся одной из основных причин успешных атак. По отчёту Group-IB, около 65 % всех инцидентов в 2024 году были вызваны действиями сотрудников — случайными или умышленными [13].

Типичные ошибки пользователей:

- открытие фишинговых писем;
- установка подозрительных приложений;
- передача логинов и паролей;
- использование личных устройств в корпоративной сети.

Согласно статистике Kaspersky и Positive Technologies, значительная часть российских компаний до сих пор не внедрила базовые элементы защиты, что демонстрирует таблица 3.

Таблица 2.3 – Уровень защищённости организаций в РФ (по данным на 2024 год)

Категория	Доля организаций (%)
Имеют систему мониторинга инцидентов (SOC)	32
Проводят регулярные аудиты ИБ	45
Имеют план реагирования на киберинциденты	41
Обучают сотрудников основам ИБ	39

Эти данные показывают, что даже в условиях роста угроз значительная доля организаций пренебрегает системной работой в области ИБ. Отсутствие регулярных аудитов, обучения и систем мониторинга создаёт благоприятную среду для атак.

Анализ текущего состояния ИБ в цифровой экономике демонстрирует нарастающее несоответствие между уровнем угроз и готовностью к ним большинства организаций. Проблема усугубляется слабой культурой безопасности, недостатком подготовки персонала и нехваткой финансовых ресурсов на внедрение современных систем защиты. Это делает необходимым переход к системному управлению информационной безопасностью, ориентированному на проактивную модель, постоянный мониторинг, обучение и устойчивость к инцидентам.

2.2 Современные подходы и технологии обеспечения ИБ

Современные подходы к обеспечению информационной безопасности (ИБ) развиваются в условиях растущей цифровизации, усложняющихся киберугроз и необходимости защищать не только данные, но и бизнес-процессы, инфраструктуру и цифровую идентичность субъектов. Одним из важнейших факторов в этом процессе становится отход от традиционной периметральной модели защиты, в которой доверие предоставляется автоматически при нахождении внутри корпоративной сети. Новые подходы основываются на управлении рисками, постоянной верификации, прогнозировании поведения и вовлечении всех уровней организационной структуры в обеспечение ИБ.

Наиболее активно внедряемой концепцией в последние годы стала архитектура нулевого доверия (Zero Trust Architecture). Она опирается на фундаментальное допущение, согласно которому ни один пользователь, устройство или система не может быть априори признанными надёжными. Все действия, независимо от источника, подлежат контролю, а доступ к ресурсам предоставляется строго в рамках минимально необходимого уровня. Такая модель делает невозможным автоматическое перемещение злоумышленника внутри сети даже в случае получения им начального доступа. Внедрение принципов Zero Trust позволяет снизить уязвимость к атакам на основе компрометации учетных данных, минимизировать последствия инсайдерских инцидентов и адаптироваться к условиям удалённой работы и гибридной ИТ-инфраструктуры. В России элементы архитектуры нулевого доверия активно внедряются с 2021 года, особенно в госсекторе и критически важных отраслях, что отражено в рекомендациях ФСТЭК и Минцифры РФ.

Вторым ключевым направлением является формализация процессов обеспечения ИБ через внедрение систем управления информационной безопасностью (ISMS). Эти системы разрабатываются на основе международных стандартов серии ISO/IEC 27000, в частности ISO/IEC

27001:2022, и предполагают создание замкнутого цикла управления безопасностью: от выявления рисков до постоянного совершенствования практик защиты. Внедрение ISMS позволяет организациям систематизировать работу с ИБ, интегрировать требования в общие бизнес-процессы, повысить уровень ответственности сотрудников и соответствовать ожиданиям партнёров и регуляторов. По данным Positive Technologies, к 2024 году в России сертифицированными по ISO/IEC 27001 являются около 24 % крупных компаний, преимущественно из банковского сектора, телекоммуникаций и IT-отрасли [6].

Развитие технологий искусственного интеллекта (AI) и машинного обучения (ML) привело к трансформации подходов к мониторингу и реагированию на киберугрозы. В рамках концепции проактивной безопасности организации всё чаще используют интеллектуальные системы анализа поведения пользователей и устройств (User and Entity Behavior Analytics — UEBA), способные в реальном времени выявлять аномалии, указывать на потенциальные инциденты и автоматически инициировать меры реагирования. Такие технологии существенно повышают эффективность работы центров мониторинга информационной безопасности (SOC), позволяют ускорить обнаружение вторжений и минимизировать время реакции на атаки. Кроме того, AI-инструменты применяются для корреляции событий, фильтрации ложных срабатываний и предиктивного анализа. В 2024 году в России использование таких решений выросло на 19 % по сравнению с 2022 годом, особенно в секторе финансов и госуслуг [6].

Одним из приоритетных направлений становится защита персональных данных, особенно в контексте растущих требований законодательства. В России требования закреплены в Федеральном законе № 152-ФЗ «О персональных данных», а также в методических рекомендациях Роскомнадзора и ФСТЭК. Современные технологии обеспечения конфиденциальности включают в себя токенизацию, шифрование,

анонимизацию, а также разграничение прав доступа и использование средств защиты на этапе обработки и хранения данных. Международный стандарт ISO/IEC 27701:2019, расширяющий ISO/IEC 27001, служит основой для построения систем управления конфиденциальностью и активно используется в транснациональных корпорациях. В 2023–2024 годах отмечено увеличение числа утечек персональных данных в открытый доступ, что подтверждает необходимость совершенствования механизмов защиты в данной сфере. Так, в 2024 году в даркнете было обнаружено более 250 баз данных, содержащих информацию о пользователях российских сервисов [источник: rbc.ru, 2024].

Растущая популярность облачных технологий также требует адаптации подходов к ИБ. Обеспечение безопасности в облачных средах предполагает совместную ответственность поставщика и клиента, а также использование облачно-ориентированных средств защиты. Среди них — виртуальные фаерволы, шифрование на стороне клиента, защита API, контроль доступа на основе атрибутов и интеграция с системами мониторинга. Стандарты Cloud Security Alliance и рекомендации NIST (США) всё чаще используются российскими компаниями при переходе на облачные решения. Однако, как показывают исследования Kaspersky, более 40 % организаций в России по-прежнему используют публичные облака без должного контроля за данными и правами доступа, что повышает вероятность утечек и вторжений [4].

Ещё одним значимым направлением становится применение концепции киберустойчивости (cyber resilience). Она ориентирована не только на предотвращение инцидентов, но и на обеспечение непрерывности деятельности в случае реализации угрозы. Это включает резервное копирование, отказоустойчивые архитектуры, сценарии быстрого восстановления (disaster recovery) и планы обеспечения непрерывности бизнеса (BCP). Подход киберустойчивости особенно важен в условиях цифровой зависимости критических отраслей — энергетики, транспорта, финансов и здравоохранения.

Практика внедрения средств автоматизации реагирования на инциденты (Security Orchestration, Automation and Response — SOAR) также получила широкое распространение. Такие платформы позволяют объединить в единую систему информацию от различных источников, автоматизировать процессы классификации инцидентов, управления событиями и передачи информации между подразделениями. По данным международных опросов, компании, внедрившие SOAR, сокращают время реакции на инциденты более чем на 50 %, а также значительно уменьшают нагрузку на службы ИБ.

Наконец, важным элементом современной стратегии ИБ остаётся формирование культуры безопасности среди персонала. Обучение сотрудников основам цифровой гигиены, регулярные тесты на фишинг, повышение осведомлённости и участие в симулированных инцидентах позволяют значительно снизить вероятность успешных атак, особенно на основе социальной инженерии. По оценкам экспертов, затраты на обучение окупаются в среднем в течение одного года за счёт предотвращённых инцидентов и сокращения последствий [13].

Современная информационная безопасность представляет собой сложную систему, включающую технические, организационные и поведенческие компоненты. Эффективное её обеспечение невозможно без использования гибких моделей управления, автоматизации, междисциплинарного подхода и постоянного развития компетенций персонала. Внедрение актуальных технологий и подходов позволяет организациям не только защищать свои ресурсы, но и формировать устойчивость к новым угрозам, сохраняя доверие клиентов и соблюдая требования законодательства.

2.3 Перспективы дальнейших исследований и развития области

Информационная безопасность в XXI веке становится не просто областью технической защиты данных, а фундаментальной основой

функционирования цифровой экономики, социальной стабильности и государственного суверенитета. В условиях постоянного роста числа инцидентов, усложнения атакующих технологий и повсеместного распространения цифровых сервисов, область ИБ требует не только оперативного реагирования на текущие угрозы, но и стратегического планирования научно-технического развития. Современные вызовы поднимают вопросы, выходящие за рамки традиционной информационной безопасности, формируя новые междисциплинарные области исследования.

Одним из ключевых направлений дальнейших исследований является развитие киберустойчивости — способности ИТ-систем и бизнес-процессов функционировать и восстанавливаться даже в условиях реализовавшихся киберинцидентов. Это предполагает смещение акцента с исключительно превентивных мер на обеспечение непрерывности деятельности, быстрое реагирование и восстановление. В этой связи актуализируются научные разработки в области архитектур отказоустойчивых систем, автоматизации процессов реагирования, симуляции сценариев атак и построения гибридных систем управления ИБ. При этом киберустойчивость рассматривается как основа не только технической защиты, но и общей цифровой стабильности социально-экономических систем.

Особое внимание исследователей привлекают технологии искусственного интеллекта и машинного обучения, активно интегрируемые в процессы обеспечения безопасности. Интеллектуальные системы мониторинга поведения пользователей и устройств, предиктивная аналитика угроз, адаптивные алгоритмы принятия решений — всё это требует новых подходов к построению систем ИБ. Использование машинного обучения позволяет создавать проактивные модели, выявляющие аномалии до того, как произойдёт реальный инцидент. В то же время растёт потребность в исследованиях, направленных на защиту самих систем ИИ, поскольку они, как и любая информационная структура, подвержены уязвимостям и риску

манипуляций, в том числе через подмену обучающих выборок, атаки на вывод модели и внедрение вредоносных сценариев.

Неизбежной областью для перспективных исследований становится криптографическая защита в условиях наступления эры квантовых вычислений. Существующие криптографические алгоритмы, широко применяемые сегодня, могут быть скомпрометированы при наличии достаточной вычислительной мощности квантовых компьютеров. Это побуждает научное сообщество к разработке постквантовых криптографических протоколов, обладающих устойчивостью к новым типам атак. Квантовая криптография и протоколы распределения квантовых ключей также становятся объектами теоретических и экспериментальных исследований, требующих значительного технологического и методологического обновления.

Отдельный пласт будущих научных работ охватывает вопросы нормативно-правового регулирования в сфере ИБ. Технологическое развитие опережает нормативную базу, что создаёт правовые лакуны, особенно в области международного взаимодействия, регулирования цифровых платформ, оборота персональных данных и вопросов цифрового суверенитета. Необходимость формирования адаптивной правовой среды, способной реагировать на новые формы угроз, вызывает интерес к вопросам кибердипломатии, регулирования киберконфликтов и формализации ответственности в цифровом пространстве. Возникает запрос на развитие международного права в условиях цифровой трансформации, в том числе в контексте кибершпионажа, кибервойн и трансграничных операций в сети.

Глубокое внимание уделяется и поведенческим аспектам информационной безопасности. Несмотря на технические достижения, человеческий фактор продолжает оставаться одной из главных причин успешных кибератак. Эффективность социальной инженерии, рост фишинговых атак, утечки данных по вине сотрудников поднимают проблему

формирования культуры информационной безопасности. В связи с этим растёт интерес к когнитивным и социопсихологическим исследованиям, направленным на изучение цифрового поведения пользователей, факторов мотивации соблюдения правил безопасности, восприятия рисков и реакции на угрозы. В этом направлении востребованы исследования в области киберпсихологии, цифровой педагогики и построения систем поведенческой аналитики.

Вопрос кадрового дефицита в сфере ИБ остаётся острым. Согласно данным Минцифры РФ, к 2024 году нехватка квалифицированных специалистов в области кибербезопасности превысила 60 тысяч человек. Этот дефицит стимулирует развитие новых форм подготовки кадров, включая дистанционные программы, модели непрерывного обучения, внедрение ИБ-дисциплин в школьное и вузовское образование. Также актуализируются исследования в области профессионального развития, построения траекторий роста, адаптации молодых специалистов и трансфера знаний между поколениями в условиях стремительно меняющегося цифрового ландшафта.

Особый интерес вызывают исследования на стыке информационной безопасности с другими дисциплинами. Междисциплинарные подходы позволяют выйти за пределы узкотехнической логики и рассматривать ИБ в более широком контексте. Интеграция ИБ с ESG-повесткой, цифровой этикой, правами человека, устойчивым развитием и цифровой идентичностью создаёт новое поле для научного поиска. Это требует не только новых методик, но и переосмысления самих категорий безопасности, доверия, риска и устойчивости в цифровой эпохе.

Перспективы развития информационной безопасности как научной и прикладной области охватывают широкую палитру тем — от постквантовой криптографии до социально-психологических механизмов защиты. Устойчивое развитие в этой сфере возможно только при условии активного взаимодействия научного сообщества, государственного сектора, бизнеса и

международных организаций. В новых условиях ИБ становится не только инструментом защиты, но и основой цифрового суверенитета, доверия к цифровым платформам и долгосрочной безопасности государства и общества. Научное сопровождение этих процессов требует системности, прогностичности и открытости к междисциплинарному диалогу. Только объединение усилий и интеграция знаний из разных областей позволят создавать эффективные и адаптивные решения, способные противостоять постоянно меняющимся угрозам. Таким образом, информационная безопасность становится ключевым фактором устойчивого развития цифрового общества и национальной безопасности в целом.

Заключение

В процессе прохождения учебной практики по направлению информационной безопасности в цифровой экономике была проведена комплексная аналитическая работа, направленная на осмысление актуальных проблем защиты информации в условиях стремительной цифровизации и трансформации общественно-экономических отношений. Информационная безопасность сегодня выходит за пределы исключительно технической дисциплины, становясь важнейшим элементом стратегического планирования, управления рисками и устойчивого развития цифрового общества.

В первой части отчёта были рассмотрены теоретические и методологические основы рассматриваемой темы. Установлено, что информационная безопасность в цифровой экономике включает не только защиту информации и инфраструктуры, но и формирование доверия к цифровым платформам, устойчивость к внешним и внутренним угрозам, соблюдение правовых и этических норм в обращении с данными. В условиях роста числа инцидентов, утечек данных, кибершпионажа и использования вредоносных программ обеспечение ИБ становится неотъемлемой составляющей цифровой политики государства, корпоративных стратегий и образовательных программ.

Проанализированы нормативно-правовые акты, регулирующие сферу ИБ в Российской Федерации и на международном уровне. Особое значение имеют Федеральные законы № 149-ФЗ и № 187-ФЗ, а также Стратегия развития информационного общества на 2017–2030 годы. Показано, что Россия движется в сторону системного регулирования информационной безопасности, однако актуальными остаются задачи гармонизации с международными стандартами, в частности ISO/IEC 27001 и ISO/IEC 27701. В ходе практики была достигнута цель — сформировать представление об

исследовательской логике в области ИБ и овладеть методами анализа нормативных, научных и статистических источников.

В аналитической части отчёта обоснована высокая степень актуальности проблем ИБ. Установлено, что за последние пять лет количество киберинцидентов в России выросло более чем в два раза, при этом доля атак на критическую информационную инфраструктуру и с использованием программ-вымогателей продолжает расти. Основные угрозы представлены фишингом, эксплойтами уязвимостей, социально-инженерными атаками и инсайдерскими действиями. Выявлены типичные уязвимости цифровой инфраструктуры, включая устаревшие системы, слабую аутентификацию, отсутствие сегментации и недостаточный уровень подготовки персонала.

Отдельное внимание было уделено человеческому фактору. Подтверждено, что более 60 % всех инцидентов связаны с ошибками или нарушениями со стороны сотрудников. Недостаточное внимание к обучению, культуре ИБ и осведомлённости персонала остаётся критической проблемой для большинства организаций.

В разделе, посвящённом современным подходам к обеспечению ИБ, рассмотрены архитектура нулевого доверия, системы управления информационной безопасностью (ISMS), применение искусственного интеллекта, защита в облачных и распределённых системах. Подчёркнута необходимость перехода от фрагментарной защиты к интегрированной модели, в которой ИБ включена в стратегию развития организации, бизнес-процессы и корпоративную культуру.

Анализ перспектив развития показал, что информационная безопасность становится междисциплинарной областью, охватывающей не только технологии, но и право, психологию, образование, управление. Среди перспективных направлений выделены киберустойчивость, постквантовая криптография, безопасность ИИ, правовое регулирование киберугроз, а также формирование кадрового и образовательного потенциала.

В ходе учебной практики были сформированы базовые исследовательские компетенции: навыки поиска и критического анализа источников, логико-структурирования материала, формулирования выводов и аргументации. Компетенции УК-1.1в и УК-1.3в, связанные с анализом информации и применением системного подхода, были успешно реализованы в процессе подготовки данного отчёта.

Полученные знания и навыки могут быть использованы в дальнейшем обучении, при подготовке выпускных квалификационных работ и в будущей профессиональной деятельности в сфере информационной безопасности и цифрового управления. Практика продемонстрировала необходимость постоянного обновления знаний, междисциплинарного подхода и развития аналитического мышления для эффективной работы в условиях цифровой трансформации.

Список использованных источников

1 Васильев И.А. Информационная безопасность в цифровой экономике: вызовы и перспективы // Информационное общество. – 2022. – № 3. – С. 15–20.

2 Гаврилова Т.А., Кудрявцев А.Н. Цифровая трансформация и информационная безопасность: новые подходы к защите данных // Экономика и управление. – 2022. – № 4. – С. 58–65.

3 Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 09.05.2017 № 203) // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

4 Касперская Н.В. Национальная безопасность и цифровой суверенитет в эпоху кибервойн // Национальная безопасность. – 2022. – № 1. – С. 7–13.

5 Шабанов А.В., Орлова М.Н. Современные угрозы информационной безопасности в условиях цифровизации // Информационные технологии. – 2023. – № 2. – С. 22–30.

6 Positive Technologies. Аналитический отчёт «Киберугрозы: итоги 2023 года» [Электронный ресурс]. – 2024. – URL: https://www.ptsecurity.com (дата обращения 15.04.2025).

7 Лебедев С.В. Информационная безопасность бизнеса: стратегии, методы и технологии // Менеджмент сегодня. – 2023. – № 5. – С. 33–39.

8 Колосов Д.Ю. Управление рисками информационной безопасности в цифровой среде // Вестник экономики и права. – 2023. – № 6. – С. 45–52.

9 Федеральный закон от 26.07.2017 № 187-ФЗ (последняя редакция) «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. – № 31. – Ст. 4825.

10 Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской

Федерации» (ред. от 13.06.2024) // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: http://pravo.gov.ru (дата обращения 15.04.2025).

11 Bruce Schneier. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. – New York: W.W. Norton & Company, 2023. – 320 p.

12 ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements.

13 Group-IB. Threat Intelligence Report 2023 [Электронный ресурс]. – 2024. – URL: https://www.group-ib.com (дата обращения 15.04.2025).

14 Федеральный закон от 27.07.2006 № 149-ФЗ (последняя редакция) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31. – Ст. 3448.

15 Anti-Malware. Две трети атак в 2024 году были совершены на объекты КИИ [Электронный ресурс]. – 2025. – URL: https://www.anti-malware.ru (дата обращения 15.04.2025).