

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

Информационная безопасность в цифровой
экономике

Студент
гр. БМН-22-3



М.Д. Дёмина

Руководители
канд. экон. наук, доцент



Н.Р. Паршук

канд. экон. наук,
старший преподаватель



А.А. Вертинова

Нормоконтролер
канд. экон. наук,
старший преподаватель



А.А. Вертинова

Владивосток 2023

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА ЭКОНОМИКИ И УПРАВЛЕНИЯ
ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на учебную практику по получению навыков исследовательской работы

Студент: Дёмина Мария Дмитриевна

Группа: БМН 22-3

Срок сдачи: 12.06.2023 – 24.06.2023

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 2018 года).

Руководители практики
канд. экон. наук, доцент кафедры ЭУ



Н.Р. Пашук

канд. экон. наук,
старший преподаватель кафедры ЭУ



А.А. Вертинова

Задание получил:



М.Д. Дёмина

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

Студент Дёмина Мария Дмитриевна
Фамилия Имя Отчество

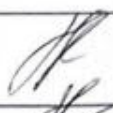
Кафедра экономики и управления гр. БМН 22-3

Руководители практики Пашук Наталья Руслановна
Фамилия Имя Отчество
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 
(подпись обучающегося)

Этапы практики	Виды работы	Срок выполнения	Отметка руководителя о выполнении
1. Подготовительный	Организационное собрание. Инструктаж по технике безопасности		
2. Исследовательский	Формулировка целей и задач исследования		
3. Аналитический	Подбор и анализ информации по теме исследования		
4. Заключительный	Подготовка и защита отчета	12.06-24.06.2023	

Руководители практики

канд. экон. наук, доцент кафедры ЭУ

 Н.Р. Пашук

канд. экон. наук,
старший преподаватель кафедры ЭУ

 А.А. Вертинова

Содержание

Введение	
1 Характеристика исследуемой проблемы по теме «Информационная безопасность в цифровой экономике»	4
2 Информационная безопасность цифровой экономики России	8
Заключение	14
Список использованных источников	15

Введение

Цель прохождения учебной практики заключается в закреплении теоретических знаний и формировании навыков исследовательской работы. Она направлена на развитие умений и навыков в проведении исследований для решения задач.

Основными задачами практики являются: закрепление теоретических знаний, формирование навыков поиска информации и развитие умения критически оценивать, обобщать и использовать полученную информацию для формулирования выводов и заключений.

Добавлю, что учебная практика является важной частью образовательного процесса, так как позволяет студентам применить полученные знания на практике и приобрести опыт в работе с реальными задачами. Кроме того, успешное прохождение практики может повысить шансы на трудоустройство после окончания учебы.

После прохождения практики студенты приобретают важную компетенцию - умение искать, критически анализировать и синтезировать информацию, а также применять системный подход для решения задач. Эта компетенция развивается благодаря поиску и анализу информации, необходимой для решения задач, а также анализу самой задачи, путем выделения ее основных составляющих.

Добавлю, что развитие компетенции поиска, анализа и синтеза информации является очень важным в современном мире, где информационные потоки неуклонно растут и становятся все более сложными. Люди, которые обладают этой компетенцией, могут быстрее и точнее находить нужную информацию, а также эффективнее использовать ее для решения задач и принятия решений. Это особенно важно в сферах науки, бизнеса, образования и государственного управления.

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

Экономическая безопасность — это состояние экономической системы, при котором она защищена от внутренних и внешних угроз, способна эффективно функционировать и обеспечивать устойчивый экономический рост и благосостояние населения. В рамках этого понятия рассматриваются такие аспекты, как защита национальных интересов, устойчивость финансовой системы, развитие конкурентоспособного производства и торговли, обеспечение социальной стабильности и т.д. Кроме того, экономическая безопасность также включает в себя защиту прав интеллектуальной собственности, борьбу с коррупцией, противодействие экономическому шпионажу и терроризму.

Информационная безопасность является важным аспектом в цифровой экономике, где все более чем когда-либо зависят от технологий и интернета, что делает их уязвимыми для кибератак. В цифровой экономике, как и в любом другом пространстве, информационная безопасность должна быть приоритетом. Это означает, что организации и частные лица должны обеспечивать защиту своих данных, как их собственных, так и своих клиентов.

Проблема информационной безопасности в цифровой экономике является крайне актуальной, поскольку с каждым годом все больше и больше информации хранится и передается через цифровые каналы связи. Это касается как личных данных, так и бизнес-информации.

Утечки данных и кибератаки становятся все более распространенными и могут привести к серьезным финансовым и репутационным потерям. В связи с этим, обеспечение безопасности данных становится приоритетной задачей для компаний и государственных организаций.

В первую очередь необходимо обратить внимание, с какими трудностями сталкивается малый и средний бизнес в процессе внедрения инновационных технологий: отсутствие методологии и исследований по вопросам интеграции инновационной цифровой экономики; низкая доступность цифровых решений для предприятий среднего и малого бизнеса, а также риски их внедрения в

уже существующий бизнес. Это приводит к значительным затратам на создание новой организационной структуры, формированию новой структуры предприятия, созданию новой структуры управления, коммуникаций и других аспектов деятельности фирмы.

Сложные условия характерны и для других субъектов экономического пространства, что означает необходимость принятия определенных мер по обеспечению информационной безопасности при интеграции в цифровую экономику. Прежде всего следует разработать стратегию обеспечения защиты конфиденциальности данных и определить источники утечки информации; а также определить ресурсы, необходимые чтобы обеспечить сохранность информации и эффективность ее использования.

Стратегия обеспечения информационной безопасности в условиях цифровой экономики содержит:

- 1 установление целей и задач обеспечения информационной безопасности;
- 2 установление принципов информационной безопасности;
- 3 распределение субъектов, отвечающих и входящих в процесс обеспечения информационной безопасности;
- 4 установление ресурсов цифровой экономики, которые будут применяться для обеспечения информационной безопасности;
- 5 проработка вариантов сокращения рисков информационных опасностей и утечек данных.

Подытожив данную главу, можно с уверенностью сказать, что данная проблема актуальна в нынешнее время, так как именно сейчас происходит резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных.

2 Информационная безопасность цифровой экономики России

В России на фоне всех экономических тенденций и в результате четвертой промышленной революции сформировалась новая модель экономической системы – цифровая экономическая модель.

Основным источником развития технологий и инноваций в цифровой экономике является деятельность предприятий сектора информационно-коммуникационных технологий (ИКТ). Подтверждением стремительного развития сферы ИКТ в России является график на рисунке 1.

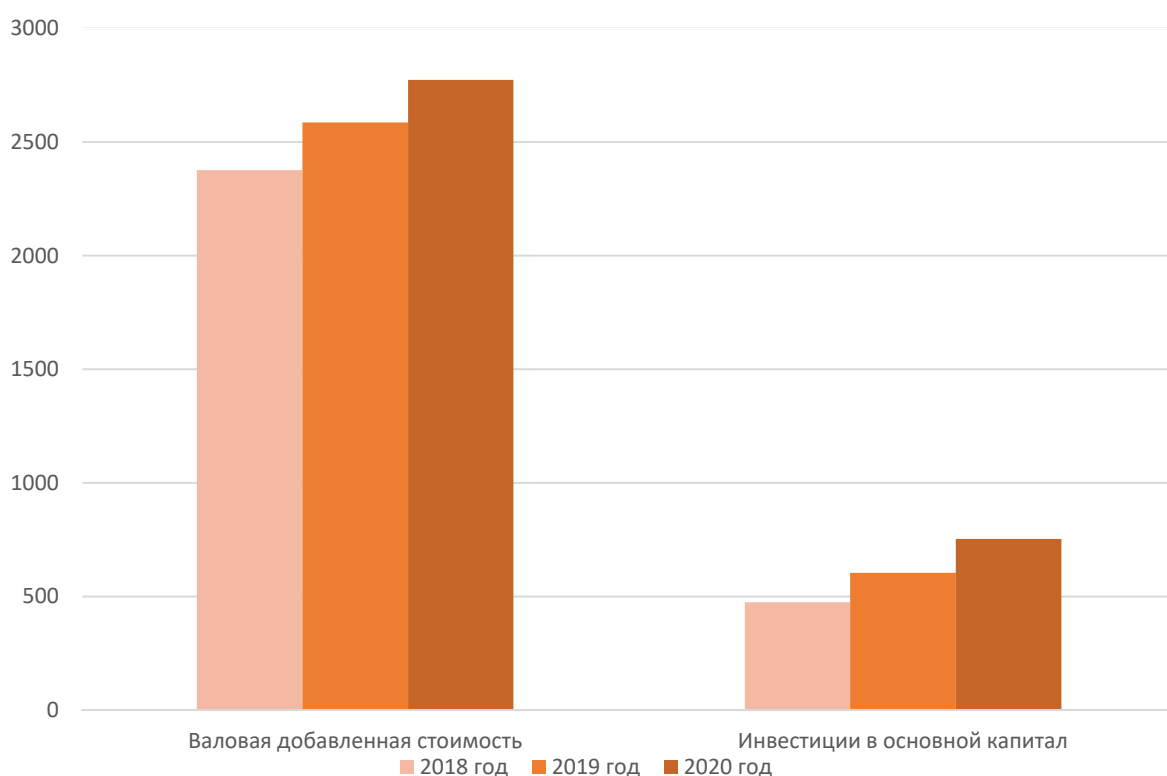


Рисунок 1 – Динамика показателя развития ИКТ в России, в млрд руб.
[2]

На диаграмме видно, что объёмы валовой добавленной стоимости увеличиваются с каждым годом, а также наблюдается увеличение капитальных вложений, что свидетельствует о стремительном дальнейшем развитии цифровой экономики в России.

Однако тенденции развития ИКТ в российской цифровой экономике связаны с угрозами и рисками от цифровой трансформации, как для деятельности

предприятий, так и государственного сектора.

Следует обратить внимание на то, что они могут выступать в качестве своеобразного троянского коня и также являются растущей угрозой.

Предотвращение возникновения имущественного ущерба в результате противоправных действий в информационной сфере.

Обеспечение информационной безопасности коммерческих организаций, некоммерческих организаций и государственных органов является одной из ключевых задач управления цифровой трансформацией [3].

Актуальность организации системы обеспечения информационной безопасности в условиях цифровой экономики России для предприятий является следующий ряд экономических преступлений, связанных с материальным ущербом от неправомерных действий в информационном поле:

- 1 Промышленный шпионаж и недобросовестные методы конкуренции.

- 2 Незаконное использование объектов интеллектуальной собственности другими экономическими субъектами, включая их кражу.

- 3 Незаконное использование конфиденциальной информации и ее кража.

По данным за 2020 г. численность хакерских атак с целью кражи информации и интеллектуальной собственности увеличилась на 51%

В российской практике все чаще наблюдается проблема обеспечения информационной безопасности организаций, из-за чего целесообразно использование различных методов и технологий. Перечислим основные из них [4]:

- 1 Биометрическая система – технологическая система, которая использует информацию о человеке для идентификации этого человека. Биометрические системы полагаются на конкретные данные об уникальных биологических признаках, чтобы работать эффективно.

- 2 Увеличение разграничения доступа для отдельных категорий сотрудников организации к определенному виду информации.

- 3 Внедрение специального режима пользования сетью Интернет.

- 4 Практическое применение программного обеспечения DLP-системы и SIEM-системы.

5 IPsec – совокупность протоколов для обеспечения информационной защиты данных, передаваемых по протоколу IP.

При этом, можно выделить следующие угрозы, которые возникают при обеспечении информационной безопасности государственного управления в условиях цифровизации экономики России:

- цифровые технологии могут выступить своеобразным «троянским ко-
нем»;
- увеличение угрозы материального ущерба от неправомерных действий
в информационном поле;
- отсутствие полноценного взаимодействия между уже созданными эле-
ментами инфраструктуры электронного правительства.

С целью обеспечения информационной безопасности государственного управления в условиях цифровизации необходимо дальнейшее развитие инсти-
тута государственной гражданской службы, путем обеспечения согласованной
работы органов власти по следующему важному направлению развития кадро-
вой политики, как обеспечении цифровизации трудовой деятельности госслу-
жащих и развитие их профессиональных компетенций . Также целесообразные
следующие решения, как:

- применение новейших цифровых технологий в системе государствен-
ного управления, как искусственный интеллект, машинное обучение и блок-
чейн;
- максимальный переход системы предоставления государственных
услуг на электронную модель.

В настоящее время в Российской Федерации существует Федеральный
закон «Об информации, информационных технологиях и о защите информа-
ции».

Рассмотрим несколько статей этого закона:

Статья 3. Принципы правового регулирования отношений в сфере ин-
формации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 16. Защита информации

1 Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления,

распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2 Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3 Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4 Владелец информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1 Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2 Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3 В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

3.1 либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

3.2 либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

4 Провайдер хостинга, оператор связи и владелец сайта в сети "Интернет" не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

5 Лица, права и законные интересы которых были нарушены владельцем социальной сети в результате неисполнения им требований, установленных в статье 10.6 настоящего Федерального закона, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации [5].

Также правительством РФ была разработана стратегия экономической безопасности.

Стратегия экономической безопасности РФ на период до 2030 года — документ стратегического планирования, разработанный в целях реализации национальных приоритетов Российской Федерации, определенных в Стратегии национальной безопасности Российской Федерации. Документ утвержден Указом Президента Российской Федерации от 13 мая 2017 года № 208 и вступил в силу со дня его подписания.

Доктрина подробно описывает базовые угрозы и вызовы экономической безопасности, а также формулирует цели, основные направления и задачи государственной политики в сфере обеспечения экономической безопасности.

Целями государственной политики в сфере обеспечения экономической безопасности являются:

- 1 укрепление экономического суверенитета Российской Федерации;
- 2 повышение устойчивости экономики к воздействию внешних и внутренних вызовов и угроз;
- 3 обеспечение экономического роста;
- 4 поддержание научно-технического потенциала развития экономики на мировом уровне и повышение ее конкурентоспособности;

- 5 поддержание потенциала отечественного оборонно-промышленного комплекса на уровне, необходимом для решения задач военно-экономического обеспечения обороны страны;
- 6 повышение уровня и улучшение качества жизни населения.

Основными направлениями государственной политики в сфере обеспечения экономической безопасности являются:

- 1 развитие системы государственного управления, прогнозирования и стратегического планирования в сфере экономики;
- 2 обеспечение устойчивого роста реального сектора экономики;
- 3 создание экономических условий для разработки и внедрения современных технологий, стимулирования инновационного развития, а также совершенствование нормативно-правовой базы в этой сфере;
- 4 устойчивое развитие национальной финансовой системы.

Подытожив данную главу, стоит отметить, что правительство Российской Федерации предпринимает множество мер по повышению эффективности прогнозирования рисков социально-экономического развития и угроз информационной безопасности в национальной цифровой экономике.

Заключение

Проблема информационной безопасности с каждым днём приобретает все большую актуальность. У злоумышленников появляется больше способов заполучить информацию.

Деятельность любой организации в наше время связана с получением и передачей информации. Информация в настоящее время является стратегически важным товаром. Потеря информационных ресурсов или завладение секретной информацией конкурентами, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству. За последние 20 лет информационные технологии проникли во все сферы управления и ведения бизнеса. Сам же бизнес из реального мира давно переходит в мир виртуальный, а поэтому весьма зависим от вирусных, хакерских и прочих атак.

Государство также вынуждено издавать законы и контролировать каналы передачи информации, чтобы защитить граждан, потому что в последнее время количество компьютерных преступлений неуклонно увеличивается, возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от обычных видов преступлений.

Так, подводя итоги, стоит отметить, что одной из наиболее уязвимых частей информационной системы являются сами пользователи. Для того, чтобы обеспечить безопасность данных, необходимо, чтобы пользователи повышали свою квалификацию и соблюдали правила информационной безопасности. Важно понимать, что защита информационной системы позволяет компании или предприятию работать безопасно и избежать убытков, связанных с ошибками в области защиты информации.

Список использованных источников

- 1 Рагимханова К. Т. Информационная безопасность в условиях цифровой экономики / К. Т. Рагимханова, З. Л. Хазбулатов, О. М. Танделова. - 2023. – С. 4-6
- 2 Абдрахманова Г.И. Цифровая экономика: 2021: краткий статистический сборник / Г.И. Абдрахманова // Нац. исслед. ун-т «Высшая школа экономики». - 2021. - С. 10-12
- 3 Зарафетдинова Э. Р. Информационная безопасность цифровой экономики России / Э. Р. Зарафетдинова // E-Scio. – 2022. – № 10. – С. 353-358.
4. Бушуев А.Л. Роль информационной безопасности в условиях цифровой экономики / Бушуев А.Л. // Baikal Research Journal. – 2020. - №1. - С. 25-27
5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция)