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-22-2 _____ С.В. Салтыкова

Руководители
канд. экон. наук, доцент _____ Н.Р. Пашук

канд. экон. наук,
старший преподаватель _____ А.А. Вертинова

Нормоконтролер
канд. экон. наук,
старший преподаватель _____ А.А. Вертинова

Владивосток 2023

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

Студент Салтыкова Софья Вячеславовна
Фамилия Имя Отчество

Кафедра экономики и управления гр. БМН-22-2

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	13.02.23-15.04.23	
2. Исследовательский	Формулировка целей и задач исследования	15.03.23-30.03.23	
3. Аналитический	Подбор и анализ информации по теме исследования	30.03.23-31.05.23	
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

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МЕЖДУНАРОДНОГО БИЗНЕСА, ЭКОНОМИКИ И УПРАВЛЕНИЯ
КАФЕДРА ЭКОНОМИКИ И УПРАВЛЕНИЯ

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

на учебную практику по получению навыков исследовательской работы

Студент: Салтыкова Софья Вячеславовна

Группа: БМН-22-2

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: _____ С.В. Салтыкова

Содержание

Введение

В современном мире, постиндустриальном обществе очень важна информация. Ее ценят, ею владеют, ее покупают и ее же могут похитить. Цифровые технологии активно входят во все сферы жизни. Доступность информационных ресурсов всем категориям граждан – от детей младшего возраста до пенсионеров – формирует представление о том, что информационные технологии способны решить абсолютно все задачи, которые волнуют современное общество. Малый и средний бизнес, некоммерческие организации проявляют активный интерес к инновациям в этой области, понимая ощутимость выгод и преимуществ от их внедрения. В современных условиях деятельность предпринимателей наполнена различными негативными факторами, связана с риском и вынужденной адаптацией к негативным и нестабильным воздействиям. С целью понижения количества перечисленных угроз и обеспечения развития предприятия необходимо создание определенной защиты от негативного влияния и воздействия внешней конкурентной среды и конкуренции внутри компании.

1 Важность информационной безопасности в цифровой экономике

Базовые идеи цифровой экономики зародились относительно недавно – в конце XX века. Исследователи до сих пор не пришли к единому мнению насчет того, что же такое цифровая экономика. Однако в большинстве случаев в определение данного понятия вкладывают следующий смысл: это виртуальная среда, дополняющая реальность системы производственных отношений. В науке существует два подхода к пониманию сущности цифровой экономики. Классический подход рассматривает цифровую экономику как экономику, в основе которой лежат цифровые технологии. При этом, данное понятие отождествляется понятиям электронных товаров и услуг, среди них медиаконтент, дистанционные образовательные технологии и другие. Расширенный подход определяет цифровую экономику как экономическое производство, связанное с использованием цифровых технологий.

Сегодня растут не только объемы виртуальных продаж, но и масштаб повсеместного распространения сферы онлайн-платежей, такие как «интернет-банкинг», электронные платежные системы, распространение криптовалют. Информационные технологии заполняют все сферы общественной жизни людей, не без исключения экономической. Они не только ускоряют и облегчают процесс обмена информацией, но и значительно повышают производительность труда. В то же время информатизация неизбежно влечет за собой риски, опасность возникновения информационных угроз, что требует более детального изучения методов информационной безопасности. Так как мы живем в эпоху цифровой экономики, нам важно понимать, как на компанию влияет ее рост и расширение.

«Цифровая экономика» относится к революционному способу взаимодействия широкой общественности и бизнеса, а также совершения транзакций в Интернете. По мере того, как известность и доступность Интернета начала расти, компании обратились к онлайн-миру как к способу добиться развития бренда и статуса в своих отраслях. Как потребители, так и предприятия начали использовать сеть Интернет для исследования продуктов, их покупки, а

также принятия решений, избегая личного общения. Сегодня хищение не останавливается антивирусным программным обеспечением. Риск кибератак постоянно растет, и для компаний это больше не вопрос «если» это произойдет, а вопрос «когда». Вот почему кибербезопасность имеет такое большое значение.

Информационная безопасность — это теория и практика предоставления доступа к информации только тем людям в организации, которые уполномочены ее просматривать. Хотя это включает в себя доступ к информации, содержащейся на компьютерах, и охватывает все записи, находящиеся под контролем организации. Когда кража данных представляет собой серьезную угрозу для личной, организационной, национальной безопасности и правительственной информации во всех областях, потребность в информационной безопасности имеет решающее значение. С последними тенденциями к большим данным во всех сферах деятельности, объем данных, связанных с государственными учреждениями и крупными организациями, огромен. Данные — это любая информация, относящаяся к личной, организационной, безопасности, оборонной, финансовой, коммерческой и другой информации во всех возможных сферах деятельности. Целями информационной безопасности является предотвращение таких утечек везде, на всех уровнях, в любое время.

2 Проблемы информационной безопасности в цифровой экономике

Цифровая экономика – это особая экономическая деятельность, основанная на цифровых технологиях, связанная с электронным бизнесом и электронной коммерцией, и производимых и сбываемых ими цифровыми товарами и услугами. На данном этапе развития экономической сферы приобретает немало важное значение электронное ведение деятельности предприятия. Оно позволяет не копить стопки бумаг, отслеживать статусы документов, а также сократить время документооборота между контрагентами.

С применением компьютерных технологий появилась возможность гораздо быстрее и удобнее обрабатывать и анализировать экономическую информацию. Компьютерная обработка экономических данных компании значительно увеличивает качественное и количественное использование информации, а также оперативность реализации операций. Многие фирмы перешли на электронный документооборот и столкнулись не только с малой степенью защищенности своих личных данных, но и с другими проблемами и трудностями. В современных условиях деятельность предпринимателей наполнена различными негативными факторами, связана с риском и вынужденной адаптацией к негативным и нестабильным воздействиям. С целью понижения количества перечисленных угроз и обеспечения развития предприятия нужно в первую очередь создать защиту от негативного влияния и воздействия внешней конкурентной среды и конкуренции внутри компании. Внутренняя составляющая экономической безопасности предприятия характеризуется такими факторами как:

–информационный фактор, то есть сбор информации из отрытых и закрытых источников;

–товарный или маркетинговый фактор (конкурентоспособность товара, услуги и их ценовая политика);

–рыночный фактор (возможности предприятия препятствовать негативным воздействиям рыночного характера экономики);

–технологический фактор (изношенность и негодность материально-технической базы);

–финансовый фактор (планирование и управление активами предприятия).

С помощью анализа и предотвращения неблагоприятного воздействия данных факторов предприятие в силах стабильно функционировать на рынке и удерживать конкурентную планку. Эти составляющие экономической безопасности помогут оперативно реагировать на всевозможные изменения и корректировать доступность личной информации. Экономическая информация, характеризующая деятельность компаний – это один из самых ценных ее активов. Важно отметить, что внешние атаки могут совершать как недобросовестные сотрудники компаний, которые работают в интересах конкурентов или бывшие сотрудники, имевшие доступ к конфиденциальным данным, а также совершенно посторонние лица. Все они придерживаются одной цели: получить конфиденциальную информацию для совершения определенных манипуляций, несущих в дальнейшем негативные финансовые и юридические последствия для компании или ее сотрудников. Например, внесение цифровых изменений в графики прибыли, что повлечет за собой причинение материального и морального вреда компании. По статистике нехватка квалифицированных и подготовленных кадров является серьезной и сложной проблемой в обеспечении информационной безопасности. В данном случае имеются в виду специалисты в аналитической и управленческой сферах. Этому способствует отсутствие должных образовательных программ, обучающих курсов и некоторая величина трудоустройства. Многие регионы отмечают нехватку специалистов или отток кадров, с недостаточными знаниями в области цифровых технологий. Необходимо запустить ряд курсов по повышению квалификации для уже работающих специалистов и выделить больше бюджетных мест в данном направлении, тогда самая важная проблема будет устранена.

Из этого вытекает вторая проблема цифровой экономики – это отсутствие должной законодательной базы, а именно нормативно-правовых актов. Одним из достаточно оперативных способов оказания различных услуг выступает переход к электронному взаимодействию с потребителями. Существующие нормативно-правовые акты не могут в точности соответствовать реальной ситуации на предприятиях, что говорит об экономической незащищенности. В Федеральном законе №152 «О персональных данных» от 27 июля 2006 года необходимо уточнить положение в разделе объемов информации, которую разыскивают без согласия субъекта и способов его деперсонализации. Персональная электронная подпись также может служить источником возникновения проблем, ведь она заменяет собственноручную подпись, которую невозможно подделать и обладает достаточной юридической силой. Электронная подпись – это цифровой аналог собственноручной подписи, предназначенной для подписи электронных документов, поступивших в организация или исходя из нее. Ее нельзя подделать, потому что она содержит криптографические алгоритмы, но завладеть достаточно просто. С развитием технологий преуспевают способы и частота совершения преступлений, связанных с кражей личных данных, в том числе и кражей электронной цифровой подписи. В случае, если она попадет в руки злоумышленников, то с ее помощью возможно совершить ряд действий, несущих негативные последствия для человека, чьи личные данные были украдены.

Чтобы обезопасить себя и сберечь свои данные необходимо придерживаться нескольких важных правил:

–не предоставлять и не оставлять сканы документов и паспортных данных в общедоступных местах;

–установить пароли на устройство, в котором содержатся данные об электронной подписи;

–выбрать надежный удостоверяющий центр для получения электронной подписи;

–обязательно блокировать источник с данными о подписи;

–установить надежную и безопасную защиту от всевозможных вирусов.

Еще одним источником потенциальных проблем, связанных с утечкой личных данных является потеря паспорта или паспортных данных. Пользователи зачастую хранят фото своих документов в галерее фотографий, что крайне небезопасно, поскольку злоумышленники могут получить доступ к персональной информации, путем взлома телефона. Передача личных данных, данных банковских карт, логинов и паролей через социальные сети и различные мессенджеры также не всегда является безопасной. Сквозное шифрование данных достаточно надежный защиты конфиденциальной информации, так как доступ к информации имеют лишь пользователи, которые состоят в переписке. Также причиной кражи личных данных может послужить взлом аккаунтов социальных сетей или получение доступа к ним злоумышленников при потере смартфона.

Цифровизация в различных сферах жизни человека несет большое количество плюсов: происходит быстрый и легкий обмен информацией между людьми, находящиеся на расстоянии друг от друга; позволяет совершать покупки, не выходя из дома; позволяет обучатся в любое удобное время; позволяет быстро и эффективно вести дела, управлять компаниями, и даже целыми отраслями. Но также в эпоху цифровизации появляется ряд проблем и опасностей, связанных с развитием преступности, пользующейся отставанием законодательной сферы в вопросах защиты населения в условиях применения цифровых технологий, и определенной наивностью, отсутствием бдительности граждан, публикующих свои личные данные и не соблюдающих простые правила информационной безопасности. Личные данные человека – не просто набор данных, который облегчает жизнь пользователя. На сегодняшний день это также потенциальный источник экономических и юридических проблем в случае, если эти данные попадают в руки злоумышленников.

2.1 Угрозы информационной безопасности в цифровой экономике

Поговорим об угрозах информационной безопасности в цифровой экономике. Для начала, нужно вспомнить о том, что такое цифровая экономика. Деятельность, которая связана с развитием компьютерных технологий, а именно – интернет-реклама, онлайн-услуги, интернет-торговля, интернет-банкинг, электронная коммерция и т.п. – это и есть цифровая экономика. Крупные корпорации, правительство, различные предприятия - все используют виртуальные процессы в рамках текущей деятельности.

Под информационной безопасностью понимается защита информации от преднамеренных или случайных воздействий, а также потенциально опасные действия, которые могут нанести ущерб владельцу информации. Поговорим об этих воздействиях. Например – копирование данных, искажение или распространение информации, ограничение доступа к информации и т.д. Угрозы делятся и классифицируются на различные типы:

1. Природа возникновения угрозы:

1.1 Естественная – воздействие на систему оказывают стихийные природные явления или же объективные физические процессы;

1.2 Искусственная – воздействует на систему человек или деятельность, связанная с ним.

2. Степень проявления:

2.1 Преднамеренная угроза. В ее основе лежит злой умысел человека. Чтобы уничтожить или похитить информацию злоумышленники разрабатывают специальные программы для хищения информации или документов, прослушивание и визуальное наблюдение и т.д.

2.2 Случайная угроза – это различные ошибки работников, сбой в работе системы, сбой в работе программного обеспечения. Источники угрозы:

2.3 Человек (утечка данных путем их разглашения, негативное воздействие на ресурсы компьютерных систем);

2.4 Природа (стихийные бедствия) – такие угрозы очень опасны для информации, т.к. влекут за собой негативные последствия – информация может безвозвратно утратиться вследствие физического разрушения компьютерных систем. Нарушаются алгоритмы работы технических устройств, случаются отказы и сбои в системах;

2.5 Программное обеспечение (различные ошибки, допущенные при разработке компьютерной системы, сбои, неправильные алгоритмы работы, заражение вирусами).

3. По степени воздействия:

3.1 Активные – меняют содержание и структуру компьютерной системы;

3.2 Пассивные – наоборот, данные не изменяются.

4. По месту расположения в системе:

4.1 Угрозы доступа к информации, которая находится в оперативной памяти;

4.2 Угрозы доступа к информации, которая находится на внешних запоминающих устройствах;

4.3 Угрозы доступа к информации, которая циркулирует в линиях связи.

Объединим все угрозы в уникальные подгруппы:

- Утечка информации;
- Мошенничество;
- Нежелательный контент
- Кибер-атаки;
- Кибер-террор;
- Несанкционированный доступ
- «Вирусы» — это программы, которые после внедрения на компьютер, способны распространяться по всей системе, т.к. создают свои копии, зачастую это негативные воздействия на систему;

3 Информационная безопасность в условиях цифровой экономики

Благодаря цифровизации появилась возможность обрабатывать огромные массивы структурированных и неструктурированных данных с использованием технологий искусственного интеллекта, нейронных сетей, виртуальной реальности и других.

Следует отметить, что в России именно государство стало инициатором внедрением цифровых технологий во всех сферах: промышленности, экономики, банковской сферы и т.д. Только после того, как в государственных структурах начали вводить данные технологии и процессы, малый и средний бизнес стал интегрироваться в данном направлении, и сейчас тотальная активизация в области цифровизации происходит во всех бизнес-структурах. Однако в секторе малого и среднего предпринимательства, отличающихся минимальным влиянием государственного воздействия, данные процессы осуществляются непосредственно по инициативе самих предпринимателей, зависят от их заинтересованности и понимания ими выгод и преимуществ.

Тем не менее, несмотря на преимущества, которые несет цифровая экономика, есть и негативные обстоятельства, которые могут ставить под угрозу многие бизнес-процессы и в том числе информационную безопасность. Именно информационная безопасность в наши дни является определяющей успешность хозяйствующих субъектов, так как защищает их стратегию развития, позволяет сохранять конфиденциальность данных, которые необходимо скрывать от конкурентов, мошенников и злоумышленников.

Информационная безопасность включает в себя широкий спектр организационно-экономических и технологических аспектов, процессов, с помощью которых возможно обеспечить сохранность информации, добиться необходимого уровня целостности имеющегося информационного пространства, а также исключить утечку данных. Каждый субъект экономического пространства заинтересован в обеспечении информационной безопасности и в интеграции в цифровую экономику.

Немало важно обратить внимание на трудности, с которыми сталкиваются предприятия малого и среднего бизнеса при внедрении инновационных инструментов цифровой экономики:

– отсутствие методологической базы и исследований в области адаптации и интеграции продуктов и технологий цифровой экономики в бизнес-процессы;

– высокая стоимость инновационных средств цифровой технологии и их малодоступность для предприятий;

– отсутствие программ кредитования и поддержки применения инновационных цифровых технологий в деятельности предприятий;

– высокие риски внедрения малоизвестных неадаптированных цифровых технологий в процессы деятельности фирмы;

– сложность процессов интеграции цифровых технологий в уже сложившиеся бизнес-процессы, что приводит к необходимости реинжиниринга, моделирования новой структуры бизнеса и, как следствие, к дополнительным затратам.

Такие сложности характерны и для других субъектов экономического пространства, что определяет необходимость принятия определенных мер по обеспечению информационной безопасности при интеграции в цифровую экономику. Прежде всего, необходимо сформировать стратегию информационной безопасности, которая определит ключевые аспекты сохранения конфиденциальности данных, обозначит источники возможной утечки и определит ресурсы для создания условий обеспечения сохранности информации и ее эффективного хранения. Стратегия обеспечения информационной безопасности в условиях цифровой экономики включает в себя:

– определение целей и задач обеспечения информационной безопасности, принципов информационной безопасности;

– выделение субъектов, ответственных и вовлеченных в процесс обеспечения информационной безопасности;

– определение ресурсов цифровой экономики, которые будут использоваться для обеспечения информационной безопасности,

– отработка вариантов снижения рисков информационных угроз и утечек данных.

Реализация данной стратегии во многом зависит от ресурсного обеспечения субъекта. Тем не менее, современные технические средства и системы обладают значительным потенциалом в решении данной задачи и это позволяет даже при ограниченных ресурсах решать задачу максимально эффективно.

Важная задача обеспечения информационной безопасности в условиях цифровой экономики также заключается в постоянном изменении и адаптации действующей системы защиты к новым условиям. Каждый день появляются новые технологии, новые ресурсы, инструменты и методы, которые в руках злоумышленников могут стать эффективным оружием для завладения информацией частных лиц или бизнес-структур. Поэтому специалисты и технологии обеспечения информационной безопасности должны быть постоянно готовы к таким атакам и вооружены самым современным оборудованием, технологиями, средствами защиты данных.

4 Практические аспекты получения знаний по обеспечению информационной безопасности

Приобретение знаний и умений обеспечения личной информационной безопасности может осуществляться разными способами. Активное развитие электронных услуг на фоне часто появляющейся в СМИ информации об утечках персональных данных и последствиях инцидентов информационной безопасности, происходящих в том числе из-за неграмотности пользователей, способствует осознанию гражданами важности данной проблемы и повышению их интереса к освоению навыков личной информационной безопасности. Представители органов власти, государственных организаций и предприятий оборонного комплекса обязаны проходить повышение квалификации по информационной безопасности в соответствии с требованиями законодательства. Круг изучаемых вопросов в первую очередь охватывает правила безопасной работы в информационных системах организации, в том числе в государственных информационных системах, на объектах критической информационной инфраструктуры и в информационных системах персональных данных. Полученные знания во многом универсальны, и способствуют формированию необходимых навыков безопасной работы пользователя с информационными технологиями и за пределами информационной среды.

В последние годы стало уделяться значительное внимание вопросам информационной безопасности и защиты персональных данных детей. Эта тематика включается в программы среднего образования, а первые знания школьники могут получить уже в начальных классах. В системе высшего и среднего профессионального образования обучающимся даются представления об используемых в профессиональной сфере информационных системах и технологиях. В стандартах большинства направлений высшего образования предусмотрены компетенции, направленные на формирование способности применять их с учетом требований информационной безопасности. Однако, как показывает опыт, вопросы личной информационной безопасности в силу

ограниченности учебного времени в вузах изучаются фрагментарно. Обучающие обычно знакомятся с аспектами информационных технологий безопасности.

Как и во многих областях знаний, эффективным способом освоения рассматриваемой проблематики являются тематические и деловые игры с применением активных форм обучения на основе сценариев, адаптированных к интересам аудитории. Для этой цели полезно использовать предварительное анкетирование слушателей, сформулировав задачи информационной безопасности в контексте ситуаций, типичных или достаточно реальных для собравшейся аудитории. Коллективное обсуждение проблемных ситуаций, отраженных в анкетах, активизирует аудиторию и позволяет выйти на реальные примеры, с которыми сталкивались пользователи, что способствует усвоению способов безопасного поведения и предотвращения небезопасных действий в будущем. Также стоит заметить, что на некоторые вопросы анкеты может не быть правильных ответов. Интерес обучающихся к обсуждаемой тематике можно поддерживать за счет использования инфографики, анимированных электронных ресурсов, где разбираются типичные ситуации в занимательной форме. Примером могут служить материалы, размещенные на ресурсах по безопасности пользователей в сети Интернет.

Нередко публикуются образовательные тесты, в которых в изображенной или словесно описанной ситуации требуется выбрать правильный вариант действий с точки зрения безопасности, при этом после совершения выбора открываются необходимые комментарии, поясняющие правильный выбор.

Созданный общедоступный электронный сервис по освоению цифровой грамотности позволяет осуществить самооценку ключевых компетенций цифровой экономики, в числе которых есть и компетенции по информационной безопасности. Однако следует заметить, что в тестах по информационной безопасности на этом ресурсе всё же немало вопросов, которые ориентированы в большей степени на специалистов, а не на пользователей даже при выборе самого простого уровня. Перспективной образовательной технологией в рассматриваемой области является проведение с использованием электронных

обучающих платформ игр, викторин, конкурсов, сценарии которых основаны на реальных ситуациях и требуют от пользователей активного применения своих знаний для достижения целей игры, которая может проводиться в командной или индивидуальной формах. Подобные форматы и сейчас активно развиваются в первую очередь для подготовки специалистов по информационной безопасности. Имеющийся опыт показывает, что при правильном подборе сценариев подобные платформы и форматы мероприятий могут быть интересны и эффективны при повышении осведомленности пользователей в сфере информационной безопасности, обучении их способам противодействия информационным угрозам с применением доступных методов и средств.

В настоящее время пользователям информационных технологий доступно немало возможностей формирования навыков безопасной работы в цифровой среде. Однако этого недостаточно для обеспечения личной информационной безопасности, поскольку основополагающая проблема – формирование персонального цифрового пространства, отвечающего частным и деловым информационным потребностям человека в цифровом мире.

4.1 Подготовка специалистов по информационной безопасности

Система высшего образования Российской Федерации и зарубежных стран в современных условиях испытывает значительные качественные изменения. Эти изменения отчетливо начали проявляться уже в последние десятилетия XX века, причем доминирующие тенденции в высшем образовании являются общими для всех развитых стран. Стоит отметить, что как раз-таки в этот период начался переход от «индустриальной» к «инновационной» экономике, основанной, в первую очередь, на производстве новой информации и новых знаний. Эти обстоятельства привели к определенному кризису образования в высших учебных заведениях, проявившемуся в неготовности быстро и эффективно адаптироваться к новым условиям. В зависимости от возможности университетов обеспечить высокий уровень образования произошла их диверсификация, явившаяся отражением объективных различий в уровне вузов. Кроме того, на первый план вышла проблема непрерывного образования, решаемая прежде всего за счет быстрого расширения системы дополнительной профессиональной подготовки. Больше всего кризисных явлений в высшем образовании пришлось на информационные направления подготовки специалистов как весьма затратные, требующие поддержания и постоянного обновления дорогостоящей материально технической базы учебного процесса. Эта ситуация парадоксальным образом наложилась на растущий дефицит квалифицированных кадров именно в сфере информационных технологий, вызванный ускоренным переходом к так называемой «цифровой экономике». Эти обстоятельства накладывают более повышенные требования к подготовке специалистов по информационной безопасности, которые на сложившемся рынке труда являются одними из самых востребованных. Обучение бакалавров и магистров в сфере защиты информации должно проводиться в соответствии с Приоритетными направлениями развития науки, технологий и техники в РФ, которые должны включать в себя обеспечение безопасности и противодействие терроризму. При подготовке необходимо учитывать, что направление

«Информационная безопасность» обладает существенной спецификой, связанной с принципиальной междисциплинарной системой образовательного процесса. Важную роль при этом составляет практическая ориентированность обучения, целью которой является удовлетворение реальных кадровых потребностей. Такая практико-ориентируемая система требует тесного взаимодействия с работодателями - профильными государственными и коммерческими организациями, правоохранительными органами, предприятиями реального сектора экономики и другими. Быстрое развитие информационной сферы, появление новых информационно-телекоммуникационных методов и устройств создает специфический и непрерывно изменяющийся рынок труда, требующий от выпускников направления «Информационная безопасность» умения адаптироваться к изменениям, происходящим в сфере защиты информации. Такие качества выпускников могут быть достигнуты за счет дисциплины обучения и серьезной фундаментальной составляющей. В силу этого учебная подготовка как бакалавров, так и магистров включает в себя следующие основные блоки:

1. правовую подготовку;
2. техническую и естественно-научную составляющие, основанные на достаточно большом объеме индивидуальной работы на лабораторных занятиях в специализированных лабораториях;
3. дисциплины «управленческого» профиля;
4. инновационные умения и предпринимательские навыки, которые обеспечиваются набором специфических дисциплин по социальному и технологическому предпринимательству, а также рядом экономических и финансовых дисциплин.

Особое значение имеет включение в образовательный процесс современной материально-технической базы. Такая база должна включать в себя сеть специализированных учебно-научных лабораторий, в том числе лаборатории безопасности информационных сетей, программно-аппаратной

защиты информации, технических средств защиты информации, а также электроники.

Учебно-методическое обеспечение теоретических и лабораторных занятий должно непрерывно обновляться в соответствии с изменениями реальных требований к специалистам по информационной безопасности. Связь с практикой осуществляется за счет непосредственного участия в образовательном процессе высококвалифицированных представителей профильных организаций и предприятий, а также в использовании их материально-технической базы. Непосредственное участие работодателей и тесное взаимодействие с ними на различных стадиях учебного процесса проявляется в разработке практико-ориентированных заданий для учащихся и в оценке их выполнения, в стажировке будущих специалистов при проведении работ технологического профиля во время производственных практик, в приобретении первичных навыков управления коллективом с помощью современных менеджерских технологий, в выполнении выпускных квалификационных работ по заданиям профильных предприятий и учреждений и т.д. Результатом такой организации подготовки специалистов являются улучшенные адаптационные возможности выпускников и их повышенная конкурентоспособность.

Заключение

На сегодняшний день личные данные человека — это не просто набор данных, который облегчает жизнь пользователя, но и также потенциальный источник экономических и юридических проблем в том случае, если эти данные попадают в руки злоумышленников. В современном мире, где очень важна информация, есть множество угроз, которые все же можно предотвратить. Для этого нужно обучить работников предприятия основам информационной безопасности и показать принципы работы вредоносных программ.

Также в эпоху цифровизации необходимо помнить, что самым уязвимым местом во всех высокотехнологичных системах защиты остается человек, а это значит, что необходимо помнить об опасностях и проявлять бдительность в защите личных данных, данных своих близких, а также информации, касающейся работы и бизнеса.

Список использованных источников

1 Ионкина, А. В. Проблемы информационной безопасности в цифровой экономике / А. В. Ионкина, А. А. Крохалев // Молодежь и наука. – 2021. – 4 с.

2 Рагимханова, К. Т. Информационная безопасность в условиях цифровой экономики / К. Т. Рагимханова, З. Л. Хазбулатов, О. М. Танделова // Экономика: вчера, сегодня, завтра. – 2023. – 7 с.

3 Назарова, Д. Важность информационной безопасности в цифровой экономике / Д. Назарова, Н. Башимова // Символ науки: международный научный журнал. – 2023. – № 5-1. – С. 84-85.

4 Андросюк, А. Б. Угрозы информационной безопасности в цифровой экономике / А. Б. Андросюк // Форум молодых ученых. – 2019. – № 1-1(29). – С. 233-236.

5 Поляков, В. В. Подготовка специалистов по информационной безопасности в условиях цифровой экономики / В. В. Поляков, В. В. Журавлева // Проблемы правовой и технической защиты информации. – 2019. – № 7. – С. 39-41.