

Информационная безопасность в условиях глобальной цифровизации



Петренко С.Н., д.э.н., профессор
Бессарабов В.О., к.э.н., доцент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

К ВОПРОСУ О СОСТАВЛЯЮЩИХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Процесс активной цифровизации экономики меняет не только подходы к обеспечению экономической безопасности предпринимательской деятельности, но и, прежде всего, влияет на ее составляющие. Особое значение для диагностики экономической безопасности предпринимательской деятельности имеет выделение ее составляющих, которое, по нашему мнению, должно основываться на сфере возникновения соответствующих угроз.

Так, следует подчеркнуть, что многие ученые составляющие экономической безопасности предпринимательской деятельности не связывают с соответствующими ее угрозами. В таком случае нередко происходит дублирование составляющих по своему содержанию или, наоборот, игнорирование отдельных угроз. Такой вывод сделан на основании анализа специальной экономической литературы (среди значительного количества исследований стоит выделить публикации [1-4]), затрагивающей вопросы составляющих экономической безопасности предпринимательской деятельности.

Трудно согласиться с мнением ряда ученых о необходимости выделения научно-технической, социальной, экологической, ресурсной, силовой, логистической составляющих экономической безопасности, так как они являются производными от финансовой, политико-правовой, интеллектуально-кадровой, технико-технологической, информационно-цифровой. Например, по мнению Яровой Ю.А. и Артеменко Л.П., социальная составляющая экономической безопасности сводится к «...удовлетворению материальных и нематериальных нужд работников» [4, с. 260], оставляя тем самым вопрос о сущности интеллектуально-кадровой составляющей. Очевидно, что удовлетворение таких нужд работников происходит вследствие оплаты их труда, величина которой устанавливается, исходя из их профессиональных (в т.ч. интеллектуальных) способностей. Другими словами, первопричиной социальной составляющей является интеллектуально-кадровая.

В свою очередь, экологическая составляющая, которая заключается в «...способности осуществлять деятельность в соответствии с технико-экологическими нормами» [4, с. 90], неразрывно связана с техникой и технологиями, применяемыми предпринимательскими структурами (речь идет о технико-технологической составляющей).

Такие параллели можно провести со многими выделенными составляющими экономической безопасности предпринимательской деятельности. Именно поэтому мы склонны полагать, что наиболее емкими по смысловой нагрузке составляющими экономической безопасности являются: финансовая, политико-правовая, интеллектуально-кадровая, технико-технологическая, информационно-цифровая. Прежде, чем рассмотреть указанные составляющие, акцентируем внимание на том, что полное влияние субъекты предпринимательской деятельности имеют только над интеллектуально-кадровой и технико-технологической составляющими, ограниченное – финансовой и информационно-цифровой, а политико-правовая, как правило, не подконтрольна им.

Учитывая тот факт, что зачастую решающее значение для укрепления рыночных позиций и, соответственно, развития предпринимательской деятельности имеет расширенное воспроизводство, а также выгодное размещение свободных финансовых ресурсов, финансовая составляющая, по нашему мнению, является основополагающей для экономической безопасности. Именно финансовая составляющая корректирует интересы и потенциал развития субъекта предпринимательской деятельности.

Финансовая составляющая экономической безопасности предпринимательской деятельности, собственно, как и любой другой, имеет важное значение для ее развития, так как связана с формированием таких показателей, как: финансовой автономии, покрытия и т.п. Особенностью данной составляющей для предприятий является то, что финансовое планирование находится только на стадии становления, так как в современных нестабильных условиях выполнить плановые показатели в полной мере является проблематичным.

Политико-правовая составляющая экономической безопасности предпринимательской деятельности связана с соответствующей государственной политикой. В то же время данная составляющая связана с соблюдением положений законодательства в сфере предпринимательской деятельности. Нельзя не отметить, что сейчас в Донецкой Народной Республике складывается неоднозначная ситуация с обеспечением экономической безопасности предпринимательской деятельности: стратегические документы декларируют необходимость противодействия мошенничества в предпринимательских структурах и обеспечение их экономической безопасности, но четкие, а самое главное, комплексные государственные программы отсутствуют. Кроме того, интеграция с Российской Федерацией требует постоянной корректировки нормативно-правовой базы по вопросам регулирования предпринимательской деятельности, что не всегда положительно сказывается на экономической безопасности, так как не учитывает всю ее

специфику в условиях как экономической блокады с стороны Украины, так и снижения покупательной способности юридических и физических лиц.

Интеллектуально-кадровая составляющая экономической безопасности предпринимательской деятельности связана с качественным и количественным составом кадрового обеспечения субъектов предпринимательской деятельности. Главной особенностью интеллектуально-кадровой составляющей является то, что она также связана с привлечением опытных специалистов по обеспечению экономической безопасности.

Сущность технико-технологической составляющей экономической безопасности предпринимательской деятельности связана со способностью выполнять функции операционной деятельности (производство готовой продукции, продажа товаров или оказание услуг). Кроме того, современные стандарты качества продукции также выдвигают ряд требований к технике и технологии производственного процесса. В рамках данной составляющей речь должна идти и об инновационных технологических решениях, применение которых повышает уровень экономической безопасности субъектов предпринимательской деятельности.

Особое значение в современных условиях имеет информационно-цифровая составляющая экономической безопасности предпринимательской деятельности. Сегодня в отечественной экономике можно наблюдать такую ситуацию: крупные субъекты предпринимательской деятельности уже адаптировались к современным реалиям, некоторые – принимают решение не адаптироваться, а диверсифицировать направления работы, отдельные – не могут адаптироваться из-за сложностей при формировании информационного обеспечения. Однако данная проблема не является новой для отечественной экономики, но в условиях ее цифровизации приобретает новый окрас.

Список используемых источников:

1. Горак А. В. Безопасность экономического развития предприятий: совершенствование сущности, факторы и критерии [Текст] / А.В. Горак // Инновации. – 2015. – № 2. – С. 128-130.
2. Довбня С.Б. Диагностика уровня экономической безопасности предприятия / С.Б. Довбня, Н.Ю. Гичова // Финансы. – 2008. – № 4. – С. 88-97.
3. Козаченко Г. В. Экономическая безопасность: сущность и механизмы обеспечения: монография / Г.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко. – К. : Либра, 2003. – 280 с.
4. Яровая Ю. А. Структура экономической безопасности предприятия в условиях кризиса / Ю.А. Яровая, Л.П. Артеменко // Экономический вестник Национального технического университета. – 2016. – № 13. – С. 257-263.

МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Автоматизация бизнес-процессов и стандартных задач — один из ключевых трендов мировой экономики. Цифровизация экономики помогает бизнесу увеличить производительность мощностей, оптимизировать бизнес-процессы и обеспечивает многие другие возможности.

Но, при этом появляются и новые угрозы — бизнес-компании становятся уязвимы к кибератакам. По темпам роста количества правонарушений киберпреступность опережает все остальные.

Цель написания работы — проанализировать источники угроз и методы защиты конфиденциальности личных и корпоративных данных, задачи информационной безопасности.

Поиск термина «конфиденциальность» в толковом словаре С. И. Ожегова не дал результатов. Этот термин появился с развитием информационных технологий.

Значение определения "конфиденциальность" в переводе с английского означает доверие и трактуется как необходимость предотвращения утечки (разглашения) какой-либо информации. С точки зрения этимологии, слово "конфиденциальный" происходит от латинского *confidentia* - доверие и в современном русском языке означает "доверительный, не подлежащий огласке, секретный".

Мы понимаем конфиденциальность как секретность, закрытость какой-либо информации.

Словосочетание “информационная безопасность” в разных контекстах может иметь различный смысл. В широком смысле, термин “информационная безопасность” подразумевает состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность — это не только сохранение и защита непосредственно самой информации, но также защита ее важнейших элементов, в том числе систем и оборудования, предназначенных для использования, сбережения и передачи этой информации. Информационная безопасность — это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая).

Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом

целесообразности применения и без какого-либо ущерба производительности организации.

Что же может представлять угрозу информационной безопасности?

Таких факторов достаточно много. Это умышленные действия конкурентов или недоброжелателей, что чаще всего встречается в больших компаниях.

Но, возможны также и умышленные или не умышленные действия самих сотрудников, которые могут быть выявлены практически на любом бизнес-предприятии или в структуре крупной финансовой компании.

Все эти факторы можно разделить на несколько видов:

1. *Угрозы от авторизованных пользователей.* Сюда входят умышленные или не умышленные (в результате халатности) действия сотрудников предприятия, работающих с информационной системой. Такие действия могут приводить к краже, уничтожению или изменению данных на серверах или рабочих станциях без какого-либо постороннего вмешательства в информационную инфраструктуру.

2. *Внешние целенаправленные атаки.* В эту группу входят действия, предполагающие несанкционированное проникновение в компьютерную сеть извне, а также DDOS атаки. (DoS – аббр. англ. *Denial of Service* – «отказ в обслуживании»). Целью таких атак, зачастую, является уничтожение или кража конфиденциальной информации, изменение алгоритмов работы сетей и оборудования, удаление данных серверов, вмешательство в системы управления бизнес-процессами. DDOS атаки ставят своей целью вызов перегрузок на каналах связи, серверах или узловых устройствах сетей, что приводит к потере функциональности или сильному снижению производительности этих систем.

3. *Компьютерные вирусы.* Именно эта группа является наиболее опасной для информационной инфраструктуры компании, так как является наиболее распространенной. Источником проникновения вируса может быть электронная почта, интернет, внешние носители информации и т.д. Результатом действий вируса может быть как кража информации (зачастую паролей доступа), так и ее уничтожение.

4. *СПАМ* – это сообщения, зачастую массовая рассылка, приходящие из не санкционированных источников. Сегодня СПАМ обрел такое распространение, что его можно смело отнести к источникам угроз информационной безопасности предприятия. Обилие СПАМА, приходящего на почтовые адреса сотрудников предприятия, может вызывать потерю важной корреспонденции, которую просто сложно найти в обилии СПАМ сообщений. Так же СПАМ может быть источником проникновения компьютерных вирусов, зачастую троянов.

5. К отдельной группе можно отнести *форс-мажорные обстоятельства*. Такие как порча оборудования в результате износа, неправильного использования или внешних факторов. Такие обстоятельства тоже могут приводить к потере данных, и их тоже необходимо учитывать в процессе проектирования системы информационной безопасности.

Возможно ли защитить себя от всех этих угроз информационной безопасности?

Рассмотрим основные методы защиты конфиденциальности информации:

Система аутентификации. Представляет собой основной метод защиты информации практически в любой сфере. Каждый пользователь в информационной структуре имеет свой личный идентификатор и уровень доступа, что позволяет ему выполнять какие-либо действия только в пределах этого уровня.

Виртуальные частные сети (VPN). Эта технология, позволяющая передавать данные используя глобальные общедоступные сети, такие как Интернет, через безопасные зашифрованные VPN тоннели. Таким образом, информация хоть и передается через глобальную сеть, однако не может быть доступна не санкционированно.

Фильтрация электронной почты. Эта система позволяет устанавливать определенные фильтры на содержимое входящей и исходящей корреспонденции. Таким образом оберегает внутреннюю сеть от проникновения нежелательных данных, в частности вирусов, а также исключает утечку определенных видов информации из внутренней сети.

Контроль работоспособности узлов. Ориентирован на постоянный мониторинг исправности и качества работы серверов, рабочих станций и сетевого оборудования. Помогает предусматривать и заранее предотвращать сбои в работе оборудования, которые могут повлечь за собой потерю информации.

Антивирусная защита. Ориентирована на предотвращение угроз со стороны компьютерных вирусов. Тесно взаимосвязана с фильтрацией электронной почты и межсетевым экраном.

Использование систем выявления слабых мест. Способствует выявлению слабых мест в системе защиты информации путем моделирования действий злоумышленника и тестирования работы системы при таких действиях.

Резервное копирование. Система резервного копирования позволяет сохранять резервные копии определенных данных, алгоритмов работы или конфигураций. Таким образом сводя к минимуму затраты времени на восстановление данных и рабочих процессов после сбоя.

Как видим, существует множество способов борьбы с угрозами конфиденциальности информации. Для каждой угрозы подбираются свои методы и процессы, которые контролируют определенные “узлы” информационной системы и предотвращают какие-либо сбои в них. Однако максимального эффекта можно добиться только применением всех этих методов в комплексе.

Список использованных источников:

1. Венгеров А.Б., «Теория государства и права. Учебник для юридических вузов» // серия: Высшее юридическое образование, Омега-L, 2017, с. 607
2. Певцова Е.А., Право. Основы правовой культуры. // 11 кл., учебник, М.: Русское слово, 2019
3. URL:<https://media-pravo.info/glossary/110>
4. URL:<https://dostup.media/confidentiality>

**Бахтояров В. В., преподаватель
Ледовских И.Н. студентка 4-го курса**

Торезский колледж Государственного образовательного учреждения высшего профессионального образования «Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики»

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

В большинстве стран стратегия цифровой безопасности принимается как целостный документ, связанный с обеспечением национальной безопасности. При этом масштабы угроз и риски выходят за пределы отдельных государств и становятся мировыми. Осознание данного факта способствует созданию рядом стран специализированных организаций для координации сетевой и информационной безопасности на национальном и международном уровне. Типовыми целями стратегий по обеспечению безопасности в цифровом пространстве являются:

- обнаружение кибератак и реагирование на них;
- предотвращение угроз;
- поддержка и разработка надежных продуктов и услуг для государственных структур;
- поддержка государственных учреждений и операторов инфраструктуры;
- содействие развитию образования в области цифровых технологий.

Для того чтобы рассмотреть проблемы, нам необходимо понять, что такое информационная безопасность и глобальная цифровизация.

Цифровые угрозы стали масштабней, что зачастую приводит к значительным финансовым, репутационным, временным издержкам. В отчете ВЭФ по глобальным рискам (The Global Risks Report, 2018) такие общемировые угрозы, как киберпреступность и кража данных расположены на третьем и четвертом месте по их значимости.

Вызовы, связанные с цифровыми технологиями, в той или иной степени обозначены в планах развития большинства государств, которые стремятся решать социально-экономические проблемы и снижать риски цифровизации путем разработки и реализации стратегий безопасности в цифровом пространстве

Цифровизация в глобальном плане является концепцией экономической деятельности, которая основана на цифровых технологиях, внедряемых в разные сферы жизни и производства. И эта концепция широко внедряется во всех без исключения странах.

Один из показателей успешной глобальной цифровизации – это открытая информация, которая меняет социальные, политические и бизнес-процессы и приводит к улучшению качества жизни.

Вместе с тем анализ состояния информационной безопасности показывает, что ее уровень не в полной мере соответствует требованиям времени. Все еще существует ряд проблем, серьезно препятствующих полноценному обеспечению

информационной безопасности человека, общества и государства. К основным проблемам данной сферы относят:

1. Современные условия политического и социально-экономического развития страны все еще сохраняют острые противоречия между потребностями общества в расширении свободного обмена информацией и необходимостью действия отдельных регламентированных ограничений на ее распространение.

2. Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в этой области. Несовершенное нормативное правовое регулирование не позволяет завершить формирование на территории РФ конкурентоспособных российских информационных агентств и средств массовой информации.

3. Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

4. Нет четкости при проведении государственной политики в области формирования информационного пространства, что создает условия для вытеснения информационных агентств, средств массовой информации с внутреннего информационного рынка, ведет к деформации структуры международного обмена.

5. Недостаточна государственная поддержка деятельности информационных агентств по продвижению их продукции на зарубежный информационный рынок.

6. Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность;

интересы общества в информационной сфере заключаются в упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении;

интересы государства в информационной сфере заключаются в создании условий для гармоничного развития информационной инфраструктуры, реализации конституционных прав и свобод человека в области получения информации.

Общие методы решения ключевых задач объединяют в три группы:

правовые;

организационно-технические;

экономические.

К правовым методам относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности являются:

создание и совершенствование систем обеспечения информационной безопасности;

усиление правоприменительной деятельности органов власти, включая предупреждение и пресечение правонарушений в информационной сфере;

совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности программного обеспечения;

создание систем и средств предотвращения несанкционированного доступа к информации и воздействий, вызывающих разрушение, уничтожение, искажение информации, изменение штатных режимов функционирования систем и средств информатизации и связи;

выявление технических устройств и программ, представляющих опасность для функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации, контроль за выполнением специальных требований по защите информации;

сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

контроль за действиями персонала в информационных системах, подготовка кадров в области обеспечения информационной безопасности;

формирование системы мониторинга показателей и характеристик информационной безопасности в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности включают в себя: разработку программ обеспечения информационной безопасности и определение порядка их финансирования;

Таким образом, мы можем наблюдать ряд проблем, связанных с информационной безопасностью в условиях глобальной цифровизации и предполагаемые пути решения.

Список используемых источников

1. Е.В. Вострецова. Основы информационной безопасности. – Екатеринбург.: ИПЦ УрФУ, 2019. – 208 с.

2. Программа «Цифровая экономика Российской Федерации». Распоряжение правительства РФ от 28 июля 2017 г. №1632-р.

**Кусков А.Е., старший преподаватель,
Михайличенко К. А., студентка 3 курса**

*ГОУ ВПО «Донецкая академия управления и государственной службы при
Главе Донецкой Народной Республики»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

В настоящее время формируется цифровая экономика на основе развития и внедрения современных цифровых технологий в деятельность населения и организаций. Широкое использование мобильных устройств, развитие Интернета и внедрение различных новых бизнес-процессов являются инновационными элементами, предназначенными для решения социально-экономических проблем как на мировом уровне, так и на уровне отдельных регионов и стран.

В условиях высокой цифровой взаимозависимости между различными субъектами хозяйствования создание защищенной информационной среды становится неотъемлемым элементом формирования устойчивой цифровой экономики. С точки зрения информационной безопасности (ИБ) наименее контролируемые областями среди множества цифровых технологий являются Интернет вещи и технологии искусственного интеллекта.

Такие компании, как Amazon, Apple и Google, уже сформировали цифровые платформы с использованием искусственного интеллекта, а социальная сеть Facebook запустила технологию DeepTech, которая позволяет распознавать тенденции поведения пользователей по сообщениям. Потенциальные преимущества этих цифровых технологий, безусловно, значительны, но их внедрение создает угрозы для безопасности личной информации населения, а малейшая утечка данных подрывает уверенность в инновациях и экономике в целом. [1]

Вопросу информационной безопасности в ДНР в последние годы уделяется большое внимание. Ведь использование цифровых технологий откроет новые возможности для экономического развития и оптимизации бизнес-процессов. Об этом заявила экс-министр экономического развития Виктория Романюк, выступая на Среднерусском экономическом форуме 2017 года (СЭФ-2017), проходившем в Курске. По словам экс-министра, государство может получить выгоду от цифровой экономики, и ДНР уже движется в этом направлении. [2]

Опасения по поводу последствий потери личной информации связаны с наличием случаев кражи данных, прямо или косвенно связанных с цифровыми технологиями. Значительное количество инцидентов связано с нарушениями политики конфиденциальности, целостности и доступности информации, лежащей в основе социально-экономической деятельности в цифровой среде. Нарушения конфиденциальности данных со временем становятся все более

обширными, частыми и сложными с точки зрения устранения их последствий. Нарушения ИБ также происходят из-за мошеннических действий организаций, которым пользователи предоставили личную информацию.

ДНР в полной мере не столкнулась с данными последствиями. Но уже стоит задуматься, чтобы в будущем не возникло проблем с обеспечением ИБ.

Для обеспечения ИБ на уровне государства необходимо создать документ «Доктрина информационной безопасности», которая будет описывать систему официальных взглядов на обеспечение государственной безопасности ДНР в информационной сфере по объектам информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет", сетей связи, информационных технологий и т.д. Для того чтобы обеспечить ИБ в торговом направлении, например, государственная электронная торговая площадка, для этого можно использовать криптографическую защиту данных и электронную подпись. Применение технологий блокчейна разрешит создавать смарт-контракты, которые в свою очередь позволят формировать контроль и предоставление информации о владении чем-либо.

Преимущества цифровых технологий значительны, но их внедрение создает угрозы безопасности личной информации населения, а малейшая утечка данных подрывает уверенность в инновациях и экономике в целом.

Однако первые шаги в этом направлении уже были сделаны. В 2019 году утвердили распоряжение «О создании межведомственной комиссии по информационной безопасности Донецкой Народной Республики». Нормативно-правовой акт разработан с целью реализации государственной политики в области информационной безопасности, координации деятельности органов исполнительной власти, органов местного самоуправления, предприятий, организаций и иных субъектов хозяйствования. [3]

На заседаниях Межведомственной комиссии будут рассматриваться проекты нормативных правовых актов в области ИБ анализ информации о реализации требований законодательства ДНР в области информационной безопасности.

В контексте формирования цифровой экономики вопросы информационной безопасности следует рассматривать не только на уровне отдельных организаций, но и на уровне государства. С точки зрения государственного регулирования предлагаются меры по обеспечению ИБ.

На начальном этапе необходимо сформировать группу экспертов на государственном уровне, которые будут разрабатывать политики информационной безопасности в рамках межотраслевого сотрудничества. Результатом работы должна стать стратегия информационной безопасности с четкими целями, задачами и планом действий по ее эффективной реализации. Разработанная стратегия должна учитывать различные специфические аспекты секторов экономики.

На следующем этапе необходимо усовершенствовать правовую базу для обеспечения информационной безопасности, а также разработать новые правовые стандарты для определенных случаев мошенничества, не предусмотренных действующим законодательством.

Далее, на основе принятой стратегии и обновленной нормативной базы в области информационной безопасности необходимо разработать и утвердить отраслевые стандарты информационной безопасности. Также важно наладить надежный сбор данных о случаях нарушения безопасности данных.

Таким образом, информационная безопасность становится все более важным фактором экономического развития ДНР. Цифровая трансформация, осуществленная во многих секторах экономики, приведет к изменению масштабов деятельности хозяйствующих субъектов и к новым рискам и угрозам, с которыми ранее не сталкивались. Развитие цифровой экономики во многом зависит от обеспечения информационной безопасности: возникновение угроз безопасности цифровых данных становится одним из основных направлений безопасности как на государственном уровне, так и на уровне отдельных организаций и общества в целом.

Список используемых источников:

1. Асаул В.В., Михайлова А.О. Обеспечение информационной безопасности в условиях формирования цифровой экономики // Теория и практика сервиса: экономика, социальная сфера, технологии. 2018. №4 (38). URL: <https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-usloviyah-formirovaniya-tsifrovoy-ekonomiki>

2. В.Романюк о цифровой экономике в ДНР. 2017. URL: <https://dnr-live.ru/romanyuk-tsifrovaya-ekonomika/>

3. Правительством создана комиссия по информационной безопасности ДНР. URL: <https://dnr-live.ru/pravitelstvom-sozdana-komissiya-po-informatsionnoy-bezopasnosti-dnr/>

Д.В. Мейдер

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПОНЯТИЙНО- ТЕРМИНОЛОГИЧЕСКИЙ АСПЕКТ

В настоящее время отдельные аспекты научных знаний систематизированы учеными различных направлений, однако вопросы взаимосвязи и взаимозависимости развития основных структурных компонентов дефиниции «информационная безопасность» не были предметом специальных исследований.

Изучение генезиса термина «информационная безопасность» и его эволюции, привело к пониманию того, что существующий понятийно-терминологический аппарат в информационной безопасности требует совершенствования, ибо возникают новые угрозы, новые модели построения

инфраструктуры информационной безопасности, новые возможности оказания услуг в сфере информационной безопасности.

Изучению концептуальных основ формирования термина «информационная безопасность» посвящены работы отечественных и зарубежных ученых, среди которых следует отметить труды Ю.А. Родичев, А.В. Бабаш, Е.К., Баранова, Д.А. Ларин, Е.А. Баранова, В.В. Бондарев, С.А. Нестеров, А.А. Бирюков и др.

Значение информационной безопасности возрастает, что связано с необходимостью предприятий всех форм собственности и, последствиями научно-технического прогресса и другими явлениями. Современные условия жизнедеятельности предприятий неразрывно связаны с угрозами информационной безопасности, с совершенствованием понятийно-терминологического аппарата в любой сфере деятельности человека. Не исключением является, и сфера развития комплекса защиты информации.

Целью является уточнение понятий «информационная безопасность» в контексте экономического развития.

Понятие «информационная безопасность» является объектом исследования и споров для представителей различных наук и профессий, а накопленные знания в различных сферах деятельности человечества, дают разные трактовки данной дефиниции, которые в целом не противоречат друг другу, а дополняют ее качественные признаки, что вызывает научный интерес.

Разработкой концептуальных подходов к определению «информационная безопасность» занимается множество ученых и профессоров различных наук. Их трактовки не противоречат друг другу и сходятся в том, что информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.

Термин «информационная безопасность» возник с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путем воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума.

Проведя анализ сайтов по источникам происхождения получены данные касательно понятия «информационная безопасность» которое встречается в научных статьях примерно 2 130 000 раз, в свою очередь, термин «Информационная безопасность» встречается в статьях всего 499 000 раз.

Цели современной информационной безопасности заключаются в обеспечении сохранности ключевых характеристик информации и обеспечивает:

- конфиденциальность данных;
- доступность информации;
- целостность информации;
- подлинность информации;
- недоказуемость информации.

Данные параметры дают возможность гарантировать защиту данных от внешних и внутренних угроз.

Следует подчеркнуть, что несмотря на различные трактовки дефиниции Информационная безопасность, ее главные составляющие – это обеспечение защиты любых видов информации.

В генезисе информационная безопасность XX в. выделяются несколько исторических этапов:

1935 г. – идея информационная безопасность как инструмент снижения угроз с помощью организационных и технических мер защиты, пример тому разработка защиты радиолокационных средств от воздействия на них активных маскирующих и пассивных имитирующих радиоэлектронные помехи устройств.

1946 г. – период создания ПК и внедрением в практическую деятельность. В этот период информационная безопасность была направлена на ограничения физического доступа к оборудованию.

1973 г. – образования сообществ людей, называемых «Хакеры», целью которых являлось нанесение ущерба информационной безопасности конкретных людей, организаций, стран. Информация как ресурс стала одной из важнейших составляющих государства и обеспечение безопасности этого ресурса вышло на передний уровень.

1985 г. – связан с созданием глобального информационного пространства с использованием космических средств обмена информацией, в этот момент информационная безопасность потребовала создания макросистем информационной защиты.

Информационную безопасность, как объект исследований можно разделить на категории. Данная дефиниция рассматривается учеными, как:

- наука, или научное направление;
- наука и практика управления;
- управление;
- функция управления.

С 1999 по 2004г. прослеживается интенсивная разработка нового подхода к информационной безопасности, путем усовершенствования и дополнения старого понятия.

В список объектов изучения информационной безопасности, как науки, входит множество других потоков, например:

- экономическая сфера;
- внешнеполитическая;
- внутриполитическая;
- область образования, науки, технологий;
- судебная и правоохранительная.

Изучение различных трактовок понятия «Информационная безопасность» привело к утверждению динамичности характера данной дефиниции, и её развитие обусловлено потенциалом повышения эффективности функционирования защиты информации с помощью уже существующих и разрабатываемых механизмов.

Предложенный на основе проведенных исследований алгоритм формирования и развития дефиниции позволил уточнить ее изучаемый понятийный аппарат в части необходимости консолидации отмеченных основных условий.

Перспектива дальнейших исследований лежит в плоскости дальнейшего изучения и уточнения понятийно-терминологического аппарата в области изучения информационной безопасности.

Список используемых источников:

1. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с.
2. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.
3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.
4. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013.
5. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2017.
6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.
7. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.
8. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.
9. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

**Поляруш В.В., преподаватель высшей категории,
Безгласная Е.Н., студентка 3 курса**

*ПОУПК «Донецкий экономико-правовой
кооперативный техникум имени Н.П. Баллина»*

НЕОБХОДИМОСТЬ УСОВЕРШЕНСТВОВАНИЯ КОМПЕТЕНЦИЙ СОТРУДНИКОВ СОВРЕМЕННОЙ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОНЕЦКОЙ ПОРОДНОЙ РЕСПУБЛИКИ

Несколько десятилетий назад использование первой программы в прикладных целях дало начало процессу цифровизации. Цифровизацией будем называть все, связанное с использованием программных средств, двоичного кода, информационных технологий. Сначала с помощью программ совершались

вычисления, затем программирование распространилось на технологические процессы. Информационные технологии проникли почти во все аспекты бизнеса, и этот процесс будет продолжаться. Уже сейчас электронная торговля составляет самую большую долю экономики. Цифровизация менеджмента позволяет гибко управлять предприятием, передавая часть функций программам. Цифровая телемедицина ставит диагнозы с помощью самообучающихся нейросетей. Цифровая видеостудия снимает сериалы на основе анализа предпочтений зрителей. Цифровое такси и так далее. Аналитики предрекают, что дни бизнесов, которые не пожелают оцифровываться, сочтены.

У информационной безопасности, казалось бы, нет своего содержания, она обеспечивает нормальное функционирование основного бизнес-процесса. Но, с другой стороны, его защита – это настолько важный вопрос, что служба безопасности из вспомогательного подразделения становится чуть ли не основным. И хотя киберугрозы не несут прямого вреда здоровью людей, все же безопасность транзакций, защита от хищения, сохранность дорогостоящего оборудования – вопрос жизни и смерти предприятия. В случае взлома медицинских информационных систем существует вероятность нанесения вреда здоровью и жизни людей. А если мы в ближайшем будущем, как нам обещают аналитики, перейдем на вживляемые чипы, то опасность станет вполне осязаемой. В связи с этим именно соображения информационной безопасности могут поставить светлое цифровое будущее под вопрос.

Цифровая трансформация – это не просто передача компьютеру каких-то функций. Также далека от цифровизации и лоскутная автоматизация, когда для каждой части подбирается отдельное решение, и эти решения плохо между собой дружат. О цифровой трансформации можно говорить только в том случае, если мы получаем новое качество управления, аналитики, прогнозирования. Есть компании, которые сделали цифровизацию основой своей идеологии, это привело к переосмыслению рынка, новому отношению к клиентам, дало новые инструменты и подходы. Большинство же руководителей стремятся с помощью цифровых инструментов сделать более эффективным традиционный бизнес.

Есть несколько областей, где цифровые средства уже надежно обосновались и стали всем привычны: это бухгалтерия и финансы, управление технологическим процессом, некоторые охранные функции. Понемногу завоевывает позиции электронный маркетинг, особо продвинутые компании достигли высот по цифровому управлению продажами и отношениями с клиентами. Цифровизация информационной безопасности имеет фрагментарный характер. Собственно, сама тема информационной безопасности у нас еще довольно плохо приживается. Чаще всего дело ограничивается контролем интернет-трафика или доступа к внутренним электронным ресурсам. Тогда как именно внедрение системы информационной безопасности чаще всего позволяет говорить о цифровизации управления.

История проникновения компьютеров в нашу жизнь дала нам иллюзию всемогущества, тогда как чаще всего мы осваиваем только поверхностные возможности. Переведение процессов в электронный вид позволяет лучше понимать то, чем вы управляете. В цифровой среде каждое действие оставляет

след, нужно только собрать эту информацию, проанализировать ее и сделать выводы. Современный этап развития технологий позволяет перейти к новому уровню использования цифровых средств, но для этого требуется некоторая перестройка мозгов.

Современные службы информационной безопасности обязаны быть не просто технически подкованными в области защиты информации, но и прекрасно разбираться в смежных дисциплинах. В первую очередь, в правовых вопросах применения информационной безопасности, бизнес-менеджменте, управлении проектами и т.д. Только благодаря такой междисциплинарной компетентности они будут услышаны руководством компании и смогут получить необходимые ресурсы для развития. Разумеется, чем выше должностной уровень сотрудника, тем большими компетенциями он должен обладать. Универсальный рецепт по уровню и направленности профессиональной подготовки сотрудников служб вывести невозможно, многое зависит от профиля деятельности и размеров компании. Но есть законодательные требования, обязывающие, к примеру, сотрудников служб ИБ, занимающихся внедрением и эксплуатацией криптографических средств, пройти курсы профессиональной переподготовки по направлению «Информационная безопасность». Аналогичные требования могут вскоре появиться для ИБ-специалистов, обеспечивающих защиту промышленных систем АСУ ТП (автоматизированные системы управления технологическими процессами). Поскольку почти каждая организация в нашем государстве является оператором персональных данных, сотрудникам служб информационной безопасности желательно закончить курсы по организации защиты, которые регулярно обновляются по мере выхода новых нормативных документов. Зачастую на эти курсы приходят не только «безопасники», но и юристы, и сотрудники кадровых служб, желающие расширить свои профессиональные знания. В целом, направление обучения (по тем или иным средствам защиты информации) зависит от того, какие решения эксплуатируются у заказчика.

Список используемых источников:

1. Закон Донецкой Народной Республики. О Персональных данных. Принят Постановлением Народного Совета 19 июня 2015 года.
2. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В. В. Бондарев. - Москва: Издательство МГГУ им. Н.Э. Баумана, 2016. – 250 с.
3. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. [Текст]: учебное пособие для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 "Информационная безопасность" / Ю. А. Родичев. - Санкт-Петербург [и др.]: Питер, 2017. - 254 с.

Стрижак Т.А., ст. преподаватель
Чепелева И.А., ассистент

*ГО ВПО «Донецкий национальный университет экономики и торговли
имени Михаила Туган-Барановского»*

ОБЗОР УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Актуальность информационной безопасности требует особого отношения к цели и задаче ее обеспечения. Ранее задача гарантии безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов и разграничения доступа. В современных условиях этих технологий недостаточно, поскольку любая информация, имеющая определенную ценность, подвергается угрозе. Особым риском становится возможность перехвата управления ключевыми объектами информационной инфраструктуры. В связи с этим важным требованием обеспечения деятельности образовательного учреждения является поддержание высокого уровня информационной безопасности. Помимо защиты баз данных и предотвращения хакерских атак, важно оградить обучающихся от любых проявлений пропаганды и разного рода манипуляций. Поэтому построение системы информационной безопасности в образовательной организации должны осуществлять специалисты, которые имеют соответствующий уровень квалификации и опыт.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса. К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения ИБ. Следует исходить из того, что необходимо конструировать надежные системы информационной безопасности с привлечением ненадежных компонентов (программ) [1, с. 10-11].

В Доктрине информационной безопасности Российской Федерации информационная безопасность (ИБ) – это состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим трем группам, представленным на рисунке 1.

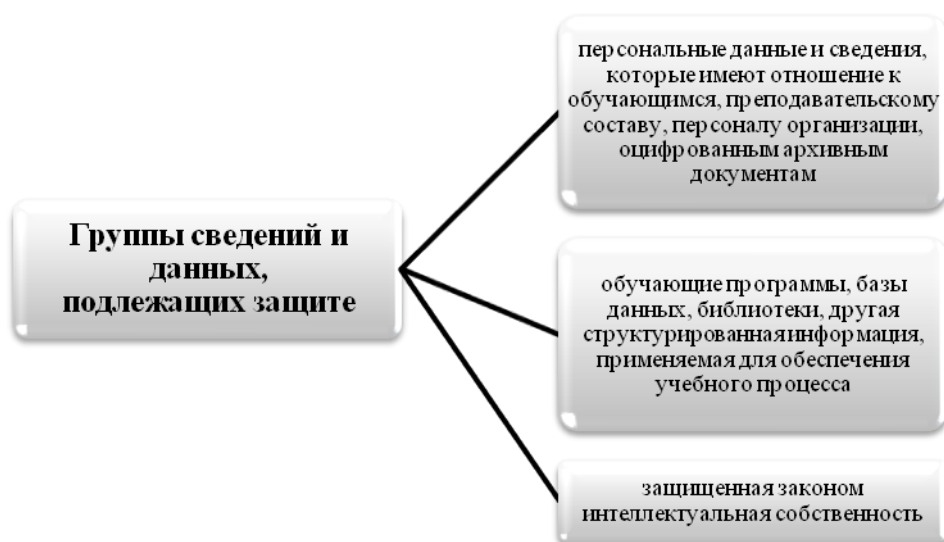


Рисунок 1 – Группы сведений и данных, подлежащих защите

Основные угрозы возникают по причине воздействия следующих факторов: несовершенство программного обеспечения и аппаратной платформы; разные характеристики строения автоматизированных систем в информационном потоке; часть процессов функционирования систем является неполноценной; неточность протоколов обмена информацией и интерфейса; сложные условия эксплуатации и расположения информации[5].

Угрозы информационной безопасности образовательного учреждения могут носить непреднамеренный и преднамеренный характер. К угрозам первого типа относятся: аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т.д.; программные сбои; ошибки работников; поломки оборудования; сбои систем связи. Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации предсказуемы, и достаточно быстро и эффективно устраняются квалифицированным персоналом.

Намного более опасными являются угрозы намеренного характера. Как правило, результаты их реализации достаточно сложно или невозможно предвидеть. Намеренные угрозы могут исходить от обучающихся, персонала организации, конкурентов и др. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов. В этих случаях легко нарушаются связи между такими удаленными компонентами, что полностью выводит систему из строя [4].

Зарубежный и отечественный опыт позволяет определить следующие наиболее распространенные угрозы информационной безопасности, которые стоят перед образовательными учреждениями [3] (табл. 1):

Исходя из краткого обзора угроз, следует, что на сегодняшний день существует более 100 позиций и разновидностей угроз информационной системе. Важно проанализировать все риски с помощью разных методик диагностики.

Таблица 1 – Угрозы информационной безопасности образовательных учреждений

Группа угроз	Краткая характеристика
Несанкционированный доступ к данным	Эта группа угроз включает в себя подмену данных в электронных журналах, архивах, хищение информации экзаменационных билетов, личных данных обучающихся и их родственников и т.п. В большинстве рекомендаций по организации схем обеспечения информационной безопасности специалисты ограничиваются только этой, технической сферой.
Фильтрация нежелательной информации	Эта группа угроз напрямую связана с противодействием экстремистской идеологии, но не ограничивается только ей. При рассмотрении угроз доступа к нежелательной информации следует также учитывать вопросы распространения провокационных материалов.
Проблемы регулирования использования социальных сетей	Именно в этой зоне осуществляется активное давление на обучающихся, запугивание, а также сравнительно новый феномен киберхулиганства.
Кибертерроризм	Несмотря на то, что эта группа угроз находится в ведении соответствующих силовых ведомств, частично она может решаться и на уровне образовательных учреждений. Создание безопасной информационно-технологической среды серьезно осложняет возможные кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматических систем и последующему повреждению инфраструктуры. Следует, впрочем, отметить, что эта группа угроз остается пока во многом гипотетической, так как учебные заведения в силу низкой их насыщенности автоматизированными управляющими системами не рассматриваются в качестве приоритетных целей для кибератак

Обеспечение и поддержка информационной безопасности образовательных учреждений включают комплекс разноплановых мер, которые предотвращают, отслеживают и устраняют несанкционированный доступ третьих лиц к информационной системе. Меры ИБ направлены также на защиту от повреждений, искажений, блокировки или копирования информации. Принципиально, чтобы все задачи решались одновременно, только в этом случае обеспечивается полноценная и надежная защита.

Список используемых источников:

1. Башлы П. Н. Информационная безопасность и защита информации: учебное пособие / П.Н. Башлы, А.В. Бабащ, Е.К. Баранова. — Москва: Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/10677.html>
2. Галатенко В. А. Основы информационной безопасности: учебное пособие / В.А. Галатенко. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/97562.html>
3. Каберник В.В. Информационная безопасность образовательных учреждений в контексте противодействия угрозам терроризма и экстремизма / В.В. Каберник // Научно-практическая конференция «Безопасность образовательной среды: противодействие идеологии терроризма и экстремизма», 9.09.2014, МГИМО
4. Информационная безопасность в образовательной организации [Электронный ресурс]. — Электрон.дан. — Режим доступа: URL:https://www.smartsoft.ru/blog/informatsionnaja-bezopasnost_v-obrazovatelnoj-organizatsii/
5. Угрозы информационной безопасности [Электронный ресурс]. — Электрон.дан. — Режим доступа: URL:<https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/>