УДК 004. 056 : 330

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭКОНОМИЧЕСКОЙ СРЕДЕ

Е.А. Зенько, О.И. Полуйчик, 3 курс
Научный руководитель – **О.В. Орешникова**, к.э.н., доцент
Полесский государственный университет

Процесс формирования глобальной информации общество развивает неуклонно возрастающими темпами. Сегодня мы становятся свидетелями широкого внедрения фундаментально новых инструментов управления экономическими системами как на уровне отдельных стран, так и в гло-

бальном масштабе. Появился новый термин «цифровая экономика», подразумевающий использование современных информационных и коммуникационных технологий (ИКТ) в обеспечении функционирования экономической системы.

При внедрении цифровой экономики становится очень важной проблема информационной безопасности, поскольку наша страна имеет слабо развитую законодательную базу по этому вопросу, а программное обеспечение, в том числе и российское, недостаточно развито. Утечка любой информации может стоить любому предприятию дорого, поэтому необходимо усиление информационной безопасности.

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Государственные и частные предприятия накапливают огромные и растущие объемы информационных активов. Предприятия и частные лица все больше полагаются на информационные и технологические активы для предоставления или приобретения товаров, услуг и информации. Предприятия и частные лица также все чаще доверяют свою информацию другим предприятиям или частным лицам. Как в странах с высоким уровнем дохода, так и в развивающихся странах люди осваивают цифровые технологии.

Глобальные прямые денежные потери от киберпреступности в 2020 году почти удвоились до 945 миллиардов долларов США с 522,5 миллиардов долларов США в 2018 году, а расходы на кибербезопасность в 2020 году, как ожидается, превысят 145 миллиардов долларов США, что в совокупности составит 1,3% мирового ВВП. Среди общего количества нарушений кибербезопасности около 95% из них вызваны человеческая ошибка.

Исследователи из школы Кларка при Университете Мэриленда являются одними из лидеров в предоставление количественной оценки хакерских атак через Интернет. В среднем каждый 39 секунд происходит хакерская атака. Большинство атак направлены на кражу имен пользователей и паролей, которые используются физическими и юридическими лицами . Среди всех атак, направленных на предприятия, 43% кибератак нападения были направлены против малого бизнеса. Между тем, компании тратят в среднем 7,68 миллиона долларов на снизить риски безопасности, связанные с кибератаками [1].

Для государственных компаний цена гораздо выше, поскольку они сталкиваются с большим количеством угроз. Средняя утечка данных на государственном предприятии оценивается в 116 миллионов долларов. Более того, наиболее распространенными методами получения личных и корпоративных данных являются: вредоносные программы (34%), мошенничество (25%), несанкционированный доступ (20%) и неправильная настройка (12%). При этом 43% компаний подвергшиеся атакам, не смогли идентифицировать эти атаки.

Информационная безопасность играет ключевую роль в обеспечении долгосрочного и успешного функционирования системы бизнеса, поскольку это способствует его защите от внешних и внутренних угроз, связанных с раскрытие информации позволяет предприятию сохранить свою репутацию и свою ценность для потенциальных инвесторы, собственники и контрагенты.

С одной стороны, информационная безопасность может быть обеспечена за счет внедрение технической службы предприятия, которая будет отвечать за информационные технологии и защита информации. С другой стороны, эффективное управление информационной безопасностью невозможно без поддержки высшего руководства, которое поймет важность этого проблемы и будет способствовать разработке на предприятии соответствующей политики и процедур для обеспечение информационной безопасности, а также понимать важность финансирования защиты информации на необходимом уровне.

На предприятиях существует прямая связь между уровнем информационной безопасности корпоративного управления и соблюдения корпоративной культуры и этического кодекса, частью которого является использование доступная сотрудникам информация по различным аспектам деятельности компании.

Источники угроз информационной безопасности делятся на внутренние и внешние. Соотношение внутренних и внешних угроз примерно 80 к 20. Внешнее включают в себя конкурентов, контрагентов, преступные группы, хакеров и другие лица, заинтересованные в информация, кото-

рая находится в распоряжении предприятия. Внутренние угрозы могут быть вызваны человеческим фактором (умышленное или неосторожное разглашение информации руководством предприятия, работниками, включая ИТ-специалистов, его утечку или несанкционированный доступ к источникам) или техническими средствами, используемыми при предприятии (программное обеспечение, электронная почта, другие средства связи).

Еще одной составляющей информационной безопасности является построение комплексной системы информационной безопасности. Защита, функционирование которой позволит защитить ее от любого случайного или целенаправленного вторжения, что может привести к его повреждению, утрате или редактированию и, как следствие, к возникновению дополнительных затрат на его возобновление или возникновение убытков, вызванных утечкой конфиденциальной информации.

К основным методам защиты информации в электронной форме относятся:

– средства идентификации пользователей и управление правами доступа позволяют администраторам контролировать действия сотрудников в системе;

– средства шифрование защищает информацию на компьютерах и в сети, делая ее перехват сложным при передаче через электронные каналы связи;

– средства антивирусной защиты;

– системы обнаружения сетевых уязвимостей и анализаторы сетевых атак;

– сетевой межсетевой экран и виртуальные частные сети [2].

Система управления информационной безопасностью должна соответствовать следующим принципам:

1. Ответственность и подотчетность – следует определить, за какую информацию каждый из сотрудников, несущий ответственность, его роль в обеспечении информационной безопасности.

2. Осведомленность о существующей корпоративной культуре на предприятии, что позволит построить отношения, основанные на взаимном доверии и тем самым исключающие существующие риски в области информационной безопасности сфера.

3. Соответствие действующим правовым актам, что позволяет обеспечить информационную безопасность на уровне предприятия без нарушения национальных или межгосударственных требований.

4. Постоянный аудит действующей системы информационной безопасности и оценка ее соответствия целей организации, что позволяет выявить существующие слабые места в процедурах, используемых для улучшения его эффективность за счет устранения существующих проблем и оплошностей [3].

В заключение отметим, что особенности информационной безопасности в экономической среде играют решающую роль в защите конфиденциальных данных и обеспечении бесперебойного функционирования бизнеса. Быстрое развитие технологий принесло множество преимуществ, но оно также подвергло организации различным киберугрозам. Поэтому предприятиям крайне важно внедрить надежные меры информационной безопасности для защиты своих ценных активов, поддержания доверия клиентов и соблюдения законодательных и нормативных требований.

Список использованных источников

1. Лойко, В. И. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. – Краснодар : КубГАУ, 2020. – 332 с.

2. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – Санкт-Петербург : Лань, 2024. – 324 с.

3. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. – Пермь : ПНИПУ, 2023. – 91с.