УДК 330

Зарубина Юлия Владимировна,
к.э.н., доцент, Ангарский государственный технический университет,
e-mail: yulzar@mail.ru
Туркин Максим Евгеньевич,
магистрант ИВТм-22, Ангарский государственный технический университет,
e-mail: jouk322@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Zarubina U.V., Turkin M.E.

INFORMATION SECURITY IN THE DIGITAL ECONOMY

Аннотация. В статье рассмотрены проблемы обеспечения защиты информации в условиях цифровой экономики, выявлены проблемы с обеспечением информационной безопасности, проведен анализ структуры преступлений в области информационных технологий, предложены меры повышения информационной безопасности.

Ключевые слова: информационная безопасность, цифровая экономика, киберпреступления.

Abstract. The article deals with the problems of ensuring the protection of information in the digital economy, identifies problems with ensuring information security, analyzes the structure of crimes in the field of information technology, suggests measures to improve information security.

Keywords: information security, digital economy, cybercrime.

В условиях растущей цифровизации экономики возрастает количество вызовов и угроз информационной безопасности, растут риски информационной безопасности. Существует несколько определений информационной безопасности. В самом общем смысле информационная безопасность – это состояние защищенности интересов различных субъектов на информированность. Также информационная безопасность – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. 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 учетом целесообразности применения и без какого-либо ущерба производительности организации. Из предложенных определений информационной безопасности вытекает сложность и многоплановость рассматриваемого понятия.

Информационная безопасность является:

- состоянием или качеством определённого объекта (объектами, включаемыми в данное определение, являются: информационная система предприятия, информация, ресурсы автоматизированной системы, данные, информационно-коммуникационная сеть);

- деятельностью, направлением которой является организация обеспе-

чения состояния защиты объекта (в этом значении чаще используется термин «защита информации», включающий в себя совокупность мероприятий правового, организационного и технического характера, направленных на предотвращение угроз информационной безопасности и на устранение их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах) [1].

Рассмотрим некоторые подходы к классификации рисков информационной безопасности. По источнику возникновения риски информационной безопасности могут возникнуть как из-за событий и явлений, не зависящих от общества, так и от случайных или умышленных событий, обусловленных обществом. Во втором случае, который наиболее интересен в разрезе данного исследования, действует «человеческий фактор»: беспечность, оплошности, недостаток опыта, умышленные противоправные действия. По содержанию риски, связанные с деятельностью людей в цифровой экономике, можно поделить на группы:

- риски нежелательного контента: приложения, рассылка, вебстраницы и материалы, запрещенные законом;

- риски несанкционированного доступа, утечки информации и потери данных;

- риски, связанные с недостаточным уровнем квалификации специалистов IT-сферы и ухода этих специалистов с отечественного рынка;

- риски низкого уровня культуры информационной безопасности. Работники не всегда осознают риски потери экономической информации;

- риски, связанные с цифровой идентификацией личности, с оцифровкой личных данных, такие как кража данных, модификация или изменение документов, кража конфиденциальной информации или коммерческой тайны, манипулирование или кража личных данных;

- риски, связанные с мошенническими действиями. К интернет-мошенничеству относят вредоносные операции с банковскими картами, взлом онлайн-банка, вымогательство и т.д.

При рассмотрении структуры киберпреступности по видам можно заметить, что интернет-мошенничество занимает большую часть числа преступлений в сфере информационных технологий [2].

Таким образом, под информационной безопасностью можно понимать защиту самой информации и защиту от информации (навязывания ложной информации). В обоих случаях проблема защиты персональных данных приобретает острый характер. Специалисты в сфере кибербезопасности прогнозируют, что к 2030 году будет более 7,5 млрд. пользователей Интернета (90 % от прогнозируемого мирового населения в 8,5 млрд) [1]. Тенденция роста киберпреступности в современном цифровом мире угрожает правопорядку, финансовой стабильности, работе государственных институтов. Рост киберпреступности сопровождается серьезными кибертеррористическими угрозами, что требует по-

иска новых подходов к обеспечению информационной безопасности. Безопасность информационных систем имеет стратегическое значение для страны, современная ситуация явно усугубляется усложнением методов и средств киберпреступлений, что требует принятия соответствующих мер.

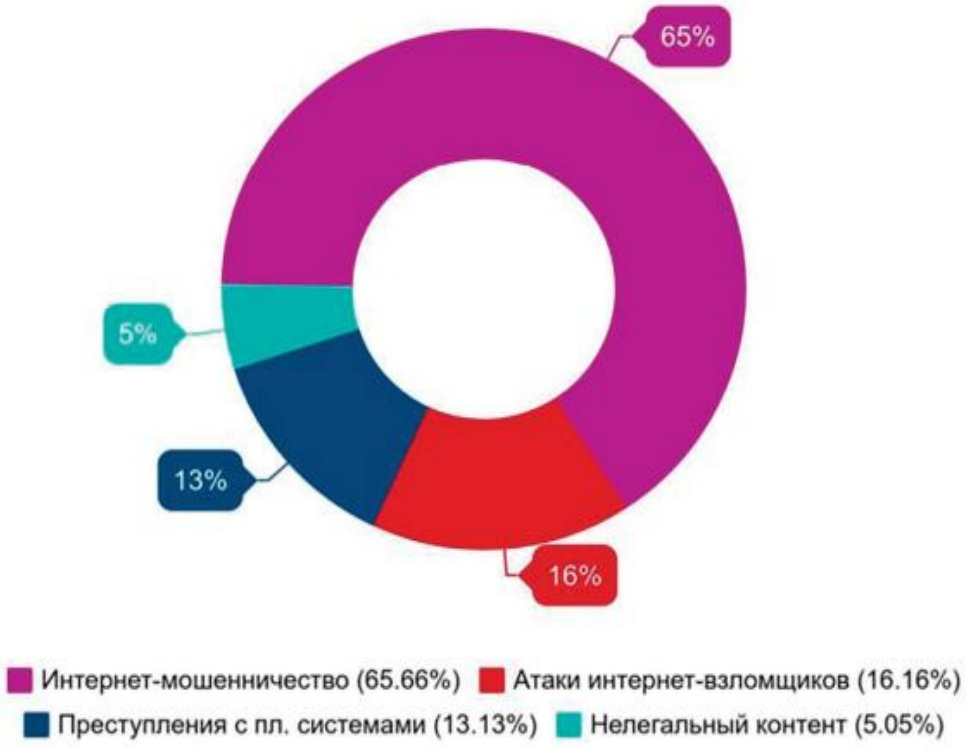

Рисунок 1 – Структура преступлений в области информационных технологий

Для повышения информационной безопасности в условиях цифровой экономики могут быть предложены следующие меры:

– регулярное оценивание уровня информационной безопасности организации, осуществление постоянного и всестороннего анализа возможных угроз и их последствий;

– усиление работы по блокировке сайтов, рассылок и call-центров мошеннических структур;

– обновление защитных программных оболочек,

– защита от нежелательного контента (антивирус, антиспам, веб-фильтры, антишпионы);

– использование фаерволов и систем обнаружения вторжений IPS;

– шифрование данных;

– использование резервного копирования.

Существенную роль в обеспечении информационной безопасности призвана сыграть программа «Цифровая экономика». В рамках этой программы, в частности, предусмотрен переход на отечественное шифровальное программ-

ное обеспечение, который потребует усилий по встраиванию российских программ шифрования в программное обеспечение, что снизит угрозы рассекречивания данных российских пользователей, хранящихся на различных интернет-ресурсах.

Важными для организации должны быть вопросы о том, созданы ли условия для внедрения современных цифровых технологий по защите информации, эффективно ли осуществляется менеджмент в сфере обеспечения информационной безопасности, насколько рационально распределены финансовые ресурсы между кадровым обеспечением задач информационной безопасности организации и цифровыми технологиями, направленными на защиту данных. Задачей государственных органов, обеспечивающих информационную безопасность, является превентивное выявление методов совершения киберпреступлений, минимизация их воздействия в случае возможного внедрения и создание условий, направленных на повышение кибербезопасности в условиях цифровой экономики.

ЛИТЕРАТУРА

1. **Левина В.И.** Информационная безопасность и угрозы информационной безопасности в коммерческих организациях / В.И. Левина. – Текст: непосредственный.// Вопросы образования и науки: сборник научных трудов по материалам международной научно-практической конференции. 2017. – С. 53-54.

2. **Суходолов А.П.** Блокчейн в цифровой криминологии: постановка проблемы / А.П. Суходолов [и др.]. – Текст: непосредственный // Всероссийский криминологический журнал. – 2019. – №4. – С. 555-563.