УДК 004

СОВРЕМЕННЫЕ УГРОЗЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Архипова С.А., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *защита информации, персональные данные, угрозы, информационная безопасность, системы, средства, персональные данные.*

В данной статье раскрыты основные понятия по теме и проведен анализ угроз персональным данным.

В условиях интенсивного развития рынка информационных продуктов и услуг, информация стала полноценным товаром, который имеет свои потребительские свойства и стоимостные характеристики. Поэтому информация, как продукт, пользуется спросом, а также требует сохранения и надежной защиты.

Персональные данные – это любая информация, непосредственно связанная с человеком, гражданином, и доверяемая им третьим лицам.

В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» [1] все организации обязаны обеспечить безопасность обрабатываемых персональных данных, причем реализовать меры защиты, соответствующие категории защищаемой информации и классу информационных систем персональных данных.

Под понятием «угроза» понимается «совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать удаление, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий» [2].

В последнее время мошенничество с данными и кибератаки являются четвертым и пятым глобальными рисками, с которыми сталкивается каждая организация. По своей значимости эти риски приравниваются к экологическим проблемам.

В официальном ежегодном отчете о киберпреступности (ACR) за 2019 год, опубликованном Cybersecurity Ventures, сообщается, что атаки хакеров во всём мире происходят каждые 14 секунд, а к 2021 году их частота возрастёт до каждой 11 секунды. Специалисты компании

InfoWatch в конце года рассказали Известиям, что за прошлый год в сеть утекло более 14 млрд. конфиденциальных записей. Рост числа утечек во всём мире по сравнению с 2018 годом увеличился на 10%, в России – более чем на 40% [3].

С развитием повсеместного проникновения интернета и роста аудитории различных сервисов, 2019 год естественным образом побил все рекорды и по количеству утекших данных и по размеру штрафов, которые накладывали на организации регулирующие органы по защите персональных данных. Киберпреступность является серьёзной угрозой для любой компании в мире и одной из самых больших проблем человечества.

К примеру, Forbes сообщил, что данные 9 млн. абонентов широкополосного доступа в Интернет от «Билайн» выложили в сеть. Сотрудники издательства, у которых подключен или был когда-то подключен интернет от «Билайна», нашли в базе свое полное ФИО, адрес, мобильный и домашний телефоны [4].

Согласно исследованию, проведенному Институтом Ponemon при финансовой поддержке Raytheon в 2018 году, выделяют 6 причин взлома данных, представим их в виде круговой диаграммы (см. рис. 1).

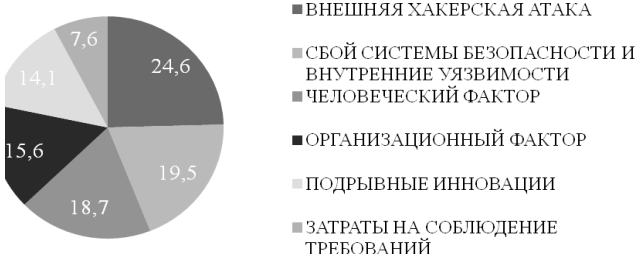

Рисунок 1 – Причины взлома данных по состоянию на 2018 г., %

Подавляющее большинство экспертов ожидают повышения частоты кибератак, ведущих к краже денег и данных (82%) и срыву операций (80%).

Одной из причин ускоренного роста киберпреступности, по мнению специалистов, являются технологические тренды. К 2022 году к интернету будет подключен один триллион устройств. К 2023 году у 80% людей появится аватар в цифровом мире. При этом более 50% интернет-трафика в 2024 году будут потреблять «умные» устройства [5].

Другой тенденцией, которую мы можем ожидать в 2020 году, станет использование искусственного интеллекта (ИИ) для борьбы с киберпреступностью. По мере того, как организации переходят от центра обработки данных к облачным платформам, использование технологий на основе ИИ будет продолжать расти и получать более широкое распространение.

Эксперты ожидают, что провайдеры облачных данных пересмотрят вопрос аутентификации и повысят уровень безопасности своих сервисов. Слишком много данных утекло с облаков в 2019 году.

Статистика показывает, что кража данных является актуальной проблемой для любой организации в мире. Интернет-мошенники с каждым днём становятся всё более опытными, и противостоять их навыкам под силу далеко не каждой компании. Но если мы как минимум будем готовы к внешнему вторжению, риск утечки данных может быть сведён к минимуму. Главное – помнить, что безопасность данных начинается с вас.

Библиографический список:

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция) // КонсультантПлюс – надёжная правовая поддержка. – URL : http://www.consultant.ru
2. Угрозы безопасности персональных данных // Практическая защита персональных данных. – URL : http://pdsec.ru
3. В 2019 году утекло вдвое больше персональных данных, чем годом ранее // InfoWatch – Информационная безопасность в цифровой экономике. – URL: https://www.infowatch.ru
4. Данные почти 9 млн абонентов «Билайна» утекли в интернет // «Forbes Russia» – финансово-экономический журнал. – URL: https://yandex.ru
5. Голубев, С. В. Информационная безопасность в автоматизированных системах управления / С. В. Голубев, С. А. Голубева, Е. А. Голубева //Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы VIII Международной научно-практической конференции молодых ученых. – Ульяновск : УлГАУ, 2017. – С. 31-34.

ANALYSIS OF THREATS TO PERSONAL DATA

Arkhipova S.A., Golubev S.V.

Key words: *information protection, personal data, threats, information security, systems, tools, personal data.*

This article describes the basic concepts on the topic and analyzes the threats to personal data.