Прокопенко Евгения Викторовна, доцент, к.физ.-мат.н., зав. каф. информационной безопасности, pev.vtit@kuzstu.ru

УДК 004.056.5;004.738.5

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПРОАКТИВНОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Н.Н. Минакова, А.В. Мансуров, А.С. Нам
Алтайский государственный университет, г. Барнаул

Ключевые слова: информационная система, персональные данные, обезличивание, двухфакторная аутентификация.

В информационной системе коммерческой организации хранится широкий спектр информации: бухгалтерская и маркетинговая информация, персональные данные сотрудников, данные о партнерах и т.д.

Законодательство по защите персональных данных постоянно совершенствуются: в 2025 году в закон о персональных данных были внесены изменения. Поэтому актуальна разработка рекомендаций для защиты персональных данных в небольших коммерческих организациях (малых предприятиях) для выбора вариантов их учета.

Представляло интерес разработать рекомендации для проактивной защиты по требованиям Федерального закона № 152 о персональных данных с изменениями 2025 года, используя встроенные возможности информационной системы малого предприятия, предположительных изменений их коммуникаций, например, анализ рынков сбыта и т.д. Предложена программа-консультант для защиты персональных данных предприятий малого бизнеса.

Изменения 2025 года закона № 152-ФЗ включают: двухфакторную аутентификацию, шифрование, требования к облачным хранилищам и антивирусам. В разработанных рекомендациях предлагается включать двухфакторную аутентификацию (2FA) через приложение – аутентификатор. В программе указаны конкретные приложения, показаны их особенности, позволяющие сделать выбор. Предложены варианты шифрования устройств, которые могут быть в информационной системе малого предприятия: ноутбуки, смартфоны, планшеты. Рекомендованы приложения, которые могут использоваться: например, для ноутбуков обязательное включение встроенного шифрования дисков, имеющегося в современных информационных системах. Разработаны критерии выбора облачных провайдеров и предложены варианты, удовлетворяющие изменениям 2025 года.

В рамках проактивной защиты в программе предусмотрен раздел по обезличиванию персональных данных. Такая необходимость у предприятия

малого бизнеса может появиться, если, например, в рамках маркетинговых исследований необходим анализ «среднего чека» по какой-либо позиции. В программе предусмотрено несколько вариантов выполнения обезличивания: метод перемешивания, метод вариации (внесения шума), метод агрегирования.

Предусмотрен раздел по защите биометрических персональных данных. Акцент сделан на возможность различных вариантов их использования: системы контроля доступа в офис с распознаванием лица, мобильное приложение для учета рабочего времени с возможностью использования селфи для отметки и т.д.

Большое внимание уделено документационному обеспечению защиты персональных данных с учетом изменений 2025 года: согласие на обработку биометрических данных, документационное обеспечение передачи персональных данных третьим лицам и т.д.

Программа построена с учетом возможностей малого бизнеса – вместо рекомендаций по использования сертифицированных средств комплексной защиты информации предлагаются бесплатные или недорогие инструменты, способные реализовать изменения 2025 года по защите персональных данных для малых предприятий: встроенное шифрование, функции табличных процессоров и т.д.

Исходные данные программы - ключевые параметры организации. К ним отнесены: вид деятельности, количество обрабатываемых записей персональных данных, используемые информационные системы (облачные, локальные базы мессенджеры), наличие биометрическим\х систем, необходимость передачи данных третьим лицам (аналитики, подрядчики).

Программа реализует интерактивный диагностический алгоритм, работающий по модульному принципу: модуль ввода параметров, аналитический модуль, модуль формирования рекомендаций и т.д.

Для обеспечения проактивной защиты:

- разработаны рекомендации как по новым обязательным требованиям (обезличивание, биометрия), так и требованиям, остающимся в рекомендательном статусе (они могут стать обязательными при изменении стратегии функционирования организации);

- выполнена интеграция правовых и технических аспектов защиты, например, рекомендации по оформлению согласий по персональным данным соединены с технической реализацией механизма их отзыва;

- рекомендации имеют контекстно-зависимый характер, связанный со спецификой бизнеса.

Разработанная программа – консультат предлагает меры по защите персональных данных для предприятий малого бизнеса не общим списком, а по принципу приоретизации: первыми в списке указаны наиболее критические действия и т.д.

Программа имеет практико-ориентированный язык: рекомендации формируются как конкретные задания (например, добавьте в форму заказа отдельную пометку для согласия на рассылку). В программе заложен механизм проверки выполнения рекомендации.

Апробация разработанного программного обеспечения показывает, что ее использование позволяет:

- сократить время приведения в соответствие требованиям по защите персональных данных с учетом современного законодательства;
- снизить финансовые затраты на защиту персональных данных за счет минимизации расходов на внешних консультантов, применения недорогих средств защиты, достаточных для выполнения требований, предъявляемых к малым предприятиям;
- реализовать проактивную защиту с учётом возможных изменений в деятельности организации.

Использование программы позволяет выявлять и устранять потенциальные проблемы по защите персональных данных, соответственно выполнять профилактику нарушении в этой области защиты информации.

Минакова Наталья Николаевна, д.ф.м.н., профессор, профессор каф. информационной безопасности, minakova@asu.ru

Мансуров Александр Валерьевич, к.ф.м.н., доцент, зав. каф. информационной безопасности, mansurov@mail.asu.ru

Нам Алина Сергеевна, студ. гр. 5.207-3, nam@mail.asu.ru

УДК 004.056

ПРИМЕНЕНИЕ СЕТЕВЫХ ОТПЕЧАТКОВ УСТРОЙСТВ ДЛЯ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ

И.С. Поздняк, Г.Н. Чифранов
ФБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», г. Самара

Ключевые слова: кибербезопасность, сетевые отпечатки, профилирование устройств, сетевые протоколы.

Важнейшим вопросом кибербезопасности в локальных сетях является предотвращение проникновения в периметр сети злоумышленников путем подключения неконтролируемых устройств. Для усиления безопасности и контроля доступа в локальной сети предлагается использовать механизмы сетевых отпечатков устройств. Внедрение технологий профилирования сетевых устройств представляет собой переход к современной архитектуре, основанной на принципах идентификации и доверии (Identity-Centric Security) [1].

Применение сетевых отпечатков позволяет добавить дополнительные факторы в процессы верификации устройств. Для этого анализируются