«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. А. И. ГЕРЦЕНА»
Институт информационных технологий и технологического образования
Кафедра информационных технологий и электронного обучения

Текст выступления по теме:

“Защита персональных данных”

Автор работы студент
2 группы 1 подгруппы
М. Н. Стецук

Санкт-Петербург
2022

1. Вступление

Здравствуйте, я студент 2-й группы 1-й подгруппы Стецук Максим. И сегодня я буду рассказывать вам о такой важной теме, как “Защита персональных данных”.

И так, приступим. Для начал, нам необходимо разобраться с главным вопросом, а именно, что такое персональные данные и какими они бывают

2. Основные понятия

Персональные данные — это любая информация, которая относится к конкретному человеку, или субъекту. ФИО, мобильный телефон, email, адрес проживания, фотография, паспортные данные – всё это является персональными данными. Важно помнить, что данные являются персональными тогда и только тогда, когда они относятся к конкретному человеку. Например, отдельно взятый номер или Email не будут являться персональными данными, вследствие отсутствия указания владельца.

Все персональные данные разделены на 4 категории:

1) Общие персональные данные:

К ним относятся базовые данные, такие как: ФИО, место регистрации, информация о месте работы, номер телефона, Email.

2) Специальные персональные данные:

К ним относится информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, информация о судимостях и тому подобное. Данная информация обычно находится в закрытом доступе.

3) Биометрические персональные данные:

Это физиологические или биологические особенности человека, которые используют для установления его личности. К ним могут относиться фотографии, отпечатки пальцев, группа крови, генетическая информация. Важно понимать, что такие данные являются биометрическими только тогда, когда используются для идентификации личности.

4) Иные персональные данные:

В эту категорию относят всё, что нельзя отнести к общедоступным, специальным или биометрическим данным.

3. Персональные данные отдельно взятых лиц

Мы живём в веке информационных технологий, вследствие чего защита персональных данных является одной из важнейших задач для компаний, организаций и даже для отдельно взятых лиц.

Для начала поговорим о персональных данных, которые могут быть украдены у отдельно взятого человека и способах их защиты.

Для чего вообще крадут такие данные?

Личные данные – недешевый товар на черном рынке. Имея базу данных, киберпреступники могут:

1) рассылать спам;

2) заражать ваши гаджеты вирусами;

3) разводить на деньги ваших друзей и знакомых;

4) заниматься фишингом (выманивать данные банковских карт и пароли);

5) отмывать деньги, украденные у других людей;

и многое другое.

Чаще всего, люди сами допускают ошибки или ведутся на обманы мошенников. Вследствие чего можно выделить 2 основных способа кражи персональных данных у обычных людей, а именно:

1) Кража сохранённых в браузере данных

Люди всё чаще совершают покупки в интернет магазинах или на интернет платформах, пользуются различными интернет ресурсами и тому подобным, где сохраняют свои данные, данные банковских карт, адреса и так далее. Эта информация шифруется браузерами, однако в связи с развитием информационных технологий, мошенники постоянно находят всё новые способы для её дешифрования и кражи.

2) Прямая просьба о предоставлении информации

Всё чаще мошенники используют этот способ. Они представляются работниками банков или сфер услуг, а также называют некоторые ваши данные, для того, чтобы вы доверились им, а затем просят предоставить ваши данные для исправления какой-нибудь ошибки или предоставления какой-либо услуги по выгодной цене. Этим они получают ещё большую информацию о конкретном человеке, для последующего её использования.

4. Рекомендации по защите персональных данных

Как же обезопасить себя от кражи персональных данных и от дальнейших проблем, которые могут возникнуть из-за этого?

1) Указывайте лишь необходимый минимум данных. Если для работы с сервисом хватит только почты и пароля, так и оставьте;

2) Используйте разные пароли для разных сервисов. Даже если утечка случится, злоумышленники не смогут раскинуть сети на все ваши аккаунты, привязанные к полученной почте. И им сложнее дальше работать, и вам проще восстановить один аккаунт вместо нескольких.

3) Настройте двухфакторную аутентификацию. Она помешает злоумышленникам получить доступ к вашим аккаунтам даже в случае, когда у них есть данные для входа;

4) При верификации на сервисе с помощью документов (паспорт, водительские права) хорошей мерой будут водяные знаки на фото или подпись на бумаге, когда и для какого сервиса было сделано фото;

5) Не используйте общедоступные хранилища для личных данных. не стоит хранить конфиденциальные данные в онлайн-службах, предназначенных для обмена информацией. Например, Google Документы — не лучшее место для файла с паролями, а сканы паспорта не надо выкладывать на Dropbox.

6) Соблюдайте осторожность в общедоступных сетях Wi-Fi. Публичные сети Wi-Fi обычно не шифруют трафик. А это значит, что кто угодно может подсмотреть, что вы отправляете и получаете, подключившись к той же точке доступа. Старайтесь не передавать через общественные сети конфиденциальные сведения: логины, пароли, данные кредитных карт и тому подобное.

5. Операторы и субъекты персональных данных

Однако, даже соблюдая эти рекомендации, персональные данные субъектов могут быть украдены, по вине операторов.

Для начала уточню, что в данном случае оператор - компания, которая собирает, хранит, обрабатывает и распространяет персональные данные, а субъект - это любой человек, персональные данные которого получил оператор.

Так как же может произойти утечка персональных данных в этом случае?

Существует 2 основных вида причин утечек данных у операторов:

1) внешние;

2) инсайдерские;

Первый вид – это неправомерное проникновение в защищённый информационный периметр организации-оператора, посредством хакерских атак.

Второй вид реализуется наиболее часто. Гражданин предоставляет сведения о себе во множестве случаев, будь то медицинское учреждение или компания, в которой он работает. Таким образом, паспортные данные, сведения о недвижимости, доходах, операциях по банковской карте оказываются в незащищенном виде, из-за чего доступ к ним становится возможным:

-при прямом проникновении недобросовестного сотрудника агентства в компьютер или к материальным носителям информации;

-при размещении их в облачных сетях, иногда на множестве серверов;

-при хищении ноутбука или портфеля сотрудника компании, в котором находится интересующая злоумышленника информация.

6. Комплексы по защите персональных данных

Так что же должны делать компании, чтобы максимально защититься от утечек персональных данных?

Основные положения о защите персональных данных в России, представлены в Федеральном законе №152-ФЗ "О персональных данных", который был принят 27 июля 2006 года.

Согласно 152-ФЗ оператор должен обеспечить защиту персональных данных, причём степень защиты зависит от типа данных:

1) Общедоступные нуждаются в самой слабой защите — их довольно легко получить, обычно их не скрывают;

2) Иные данные нужно защищать чуть сильнее — они известны меньшему кругу лиц;

3) Биометрические данные защищают еще серьезнее, поскольку их можно использовать для идентификации человека;

4) В самой серьезной защите нуждаются специальные данные — их часто можно использовать, чтобы навредить человеку.

А теперь, мне хотелось бы рассказать вам о самом комплексе мероприятий по обеспечению защиты персональных данных.

Организационные меры по защите персональных данных включают в себя:

1) Назначение лиц, ответственных за организацию обработки и обеспечение безопасности персональных данных;

2) Разработку организационно-распорядительных документов, регламентирующих весь процесс получения, обработки, хранения, передачи и защиты персональных данных;

3) Внесение изменений в бизнес-процессы организации, ознакомление пользователей, осуществляющих обработку персональных данных с положениями нормативных документов;

4) Определение перечня мероприятий по защите персональных данных и реализация таких мероприятий;

5) Осуществление внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства.

7. Заключение

На этом моё выступление подходит к концу, но прежде чем закончить, я хочу попросить вас пройти тестирование по теме моего выступления, чтобы проверить то, насколько хорошо вы усвоили рассказанную вам информацию. QR код с ссылкой на тестирование находится прямо перед вами, перейдите по нему и, заполнив информацию об отправителе, пройдите тест.

Спасибо за внимание.

Источники

1. mcs.mail.ru – Кратко и доступно: что такое персональные данные, их хранение и обработка [Электронный ресурс]. URL: https://mcs.mail.ru/blog/chto-takoe-personalnye-dannye-ih-hranenie-i-obrabotka. (Дата обращения: 20.05.22).

2. fingram26.ru – Осторожно, мошенники! Как могут украсть ваши личные данные и что с ними могут сделать [Электронный ресурс]. URL: https://fingram26.ru/articles/riski-i-finansovaya-bezopasnost/45773/. (Дата обращения: 20.05.22).

3. rb.ru – Утечки персональных данных: чем они опасны для пользователей и как от них защититься [Электронный ресурс]. URL: https://rb.ru/opinion/utechk-personalnyh-dannyh/. (Дата обращения: 20.05.22).

4. kaspersky.ru – 10 советов по защите личных данных в Интернете [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/privacy-ten-tips-2018/20898/. (Дата обращения: 20.05.22).

5. searchinform.ru – Утечка персональных данных: последствия [Электронный ресурс]. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/utechki-personalnyh-dannyh/posledstviya/. (Дата обращения: 20.05.22).

6. pointlane.ru – Защита персональных данных [Электронный ресурс]. URL: http://www.pointlane.ru/personal/. (Дата обращения: 20.05.22).