НАЦІОНАЛЬНА БЕЗПЕКА

Баньковский К.Р.
студент;
Стайкуца С.В.
кандидат философских наук, доцент;
Лемеха Т.Н.
преподаватель,
Одесская национальная академия связи имени А.С. Попова

ОБЗОР УКРАИНСКОГО IT-СЕКТОРА НА СООТВЕТСТВИЕ КРИТЕРИЯМ GDPR

С момента вступления в силу регламента по защите персональных данных (GDPR) прошло более полутора лет. Введение регламента затронуло бизнес-интересы лидеров IT-рынка Украины, действия которых для возможности дальнейшей работы на рынке Евросоюза были направлены на соответствие пунктам регламента.

Действенными примерами реализации политик GDPR являются версии сайта “ring.com” для европейских стран, “readdle.com”, “netpeaksoftware.com”.

Активные действия в сторону внедрения доработок для получения так называемого «комплайанса» (от английского слова “compliance” – соответствие) начались ещё и из-за ряда громких взысканий с больших корпораций за несоответствие требованиями GDPR. «Громким случаем» стало взыскание более чем 200 миллионов долларов с авиаперевозчика “British Airways” за использование устаревших методов защиты, из-за которых более чем 360 тысяч клиентов стали жертвами веб-скимминга. Веб-скимминг – вид мошенничества, при котором в страницу оплаты на сайте встраивается вредоносный код, который неправомерно получает платёжные данные пользователя. Также на сумму в 50 миллионов евро была оштрафована компания “Google LLC” за недостаточную прозрачность и контроль данных в вопросе обработки данных для рекламных активностей.

Размеры штрафов действительно достигают огромных цифр, потому важность обеспечения должного уровня защиты персональных данных

на современном предприятии увеличилась в разы. С появлением такого понятия как “Big Data” компании стали работать в векторе “Data-driven”, что означает принятие решений, опираясь на данные. Если такие компании не будут работать над защитой информации, тогда мы встречаемся с двумя проблемами кибербезопасности нашего времени:

– экспоненциальный рост объема данных для дальнейшей обработки;

– недостаточное количество специалистов для проведения анализа потенциальных рисков и противодействия кибератакам на данные.

Подтверждением того, что спрос на специалистов действительно растёт, является количество вакансий на сайтах для поиска работы. В Украине за 3-й квартал 2018 года было сформировано 19 вакансий специалистов по защите информации [2, с. 92], в 4-м квартале 2019 их уже 80.

Стоит отметить, что к зоне ответственности сотрудника на должности специалиста по защите информации (данных) может относиться обширный ряд вопросов. Данные вопросы охватывают организационную, правовую, социальную, программно-аппаратную и остальные сферах работы предприятия. В целом, специалист по ЗИ должен видеть «информационный образ» предприятия от «модели угроз» до конкретных регламентов, уметь описывать информационные потоки и правила работы с ними в зависимости от ситуаций, условий и должностных инструкций, защищать корпоративную информацию от утечек по всем каналам связи. И, что немаловажно, строить «культуру безопасности», основанную на критериях законности, разумности и превентивности. Более детально задачи, которые лежат в сфере компетенций специалиста по ЗИ, представлены в [3].

Примечательно, что для большинства IT-компаний требования GDPR стали привычным вопросом в любом отделе. Отдел продаж не может звонить клиентам, которые не дали на это согласия, отдел маркетинга не может отслеживать активность на сайте пользователей, которые не разрешили использовать cookie, отдел технической поддержки не может помочь решить вопрос клиента, потому что он не разрешил отправлять отчёты из программы для аналитики сервиса. Конечно, такие вопросы должны решаться более визионерски. Вся коммуникация с клиентом должна строиться в ключе доверительных отношений, а команда разработки продукта должна подтверждать доверие внедрением дополнительных мер защиты и управления персональными данными [4].

Европейский парламент считает, что только приняв системный подход как основополагающую стратегию в проектировании архитектуры защиты информации, можно в результате результата. Результата, при котором по умолчанию личные данные не были

доступны без вмешательства физического лица неопределенному числу физических лиц [5].

В целом GDPR состоит из почти сотни статей, разбитых по блокам, потому важно ознакомится с каждой из них для успешного получения “compliance”, но не нужно ставить его за цель, так как целью должно являться повышение приватности персональных данных пользователей. Основные статьи приведены на рис. 1 [1, с. 98], который построен на основе изучения документа [5].

Рис. 1. Ключевые статьи GDPR

Список использованных источников:

1. Стайкуца С. В. Работа с персональными данными в аспекте введения GDPR / С. В. Стайкуца, Т.Н. Лемеха, К.Р. Баньковский // Інноваційний розвиток науки нового тисячоліття. – 2018. – С. 97-101.

2. Баньковский К.Р. Требования к защите персональных данных клиентов в аспекте GDPR как основа кадровых изменений на рынке безопасности / К.Р. Баньковский, Т.Н. Лемеха, М.А. Лайтан, И.В. Шевченко // Матеріали четвертої всеукраїнської науково-практичної конференції «Перспективні напрями захисту інформації», ОНАЗ ім. О.С. Попова. – 2018.

3. Nate L. What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance [Електронний ресурс] / Lord Nate // Digital

Guardian. – 2018. – Режим доступу до ресурсу: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance.

4. General Data Protection Regulation [Електронний ресурс] // Wikipedia. – 2018. – Режим доступу до ресурсу:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.

5. Regulation (Eu) 2016/679 of the european parliament and of the council [Електронний ресурс] // European Parliament, Council of the European Union. – 2016.

Бордан В.Я.
ведущий специалист кафедры;
Неумытых Е.С., Сапожников А.П.
студенты,
Одесская национальная академия связи имени А.С. Попова

АНАЛИЗ АЛГОРИТМОВ РАБОТЫ СИСТЕМ ВИДЕОАНАЛИТИКИ

Видеонаблюдение (или СОТ – системы охранного телевидения, как указывается в ряде нормативных документов), как популярная подсистема безопасности, давно из «черно-белой картинки на экране монитора охранника» превратилось в интеллектуальный инструмент, нивелируя человеческий фактор. Смарт-функции современных систем видеонаблюдения базируются на системах видеоаналитики.

Программное обеспечение СОТ (детекторы) предупреждает о закрытии объектива, пересечении линии краже предметов, находит предметы в кадре, понимает, когда в кадре появляется огонь или дым, дополняя себя функциями пожарной сигнализации. Архитектура построения интеллектуальной СОТ выбирается под задачи и условия технического задания. Так, согласно [1] видеоаналитика может располагаться в камере, на сервере или присутствовать гибридным способом, когда интеллектуальные способности системы базируются и на сервере, и в пределах оконечного устройства.

Детекторы аналитики основываются на алгоритмах анализа видео. Пример рассматриваемых алгоритмов представлен на рис. 1.

Анализ движения – один из первых алгоритмов аналитики, при этом он получил большое распространение и используется практически во всех современных камерах видеонаблюдения.