СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ
SYSTEM ANALYSIS AND PROCESSING OF KNOWLEDGE

УДК 004.438 **DOI: 10.18413/2518-1092-2019-4-1-0-2**

Гончаренко Ю.Ю.
Кушнарев А.А.
Исаков С.А.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДИКИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ФГАОУ ВО «Севастопольский государственный университет»,
ул. Университетская 33, г. Севастополь, 299053, Россия

e-mail: iuliay1985@mail.ru, sahsa14.95@yandex.ru, engener1990@mail.ru

Аннотация
Наиболее актуальный и распространенный вид информации, с которым работают практически все организации Российской Федерации – это персональные данные. По причине их распространенности они требуют особой бдительности при их обработке и обеспечении безопасности. Информационные системы обрабатывающие персональные данные могут подвергаться различным атакам из-за определенных уязвимостей. Для обеспечения максимальной защищенности информационной системы персональных данных Федеральная служба по техническому и экспортному контролю разработала специальную методику для определения актуальных угроз информационной системе. Для уменьшения трудозатрат эксперта при оценке каждой угрозы актуальным будет автоматизация данного процесса, что в конечном итоге не только даст выигрыш по времени, но и сократит количество ошибок, связанных с человеческим фактором.
Ключевые слова: персональные данные; актуальные угрозы безопасности; информационная система персональных данных; модель угроз; программная реализация.

UDC 004.438

Goncharenko J.A.
Kushnaryov A.A.
Isakov S.A.

SOFTWARE IMPLEMENTATION OF THE METHOD FOR DETERMINING THE ACTUAL THREATS TO THE PERSONAL DATA SECURITY

FSAEI HE "Sevastopol state University", University street 7, Sevastopol, 299053, Russian

e-mail: iuliay1985@mail.ru, sahsa14.95@yandex.ru, engener1990@mail.ru

Abstract
The most relevant and widespread type of information that almost all organizations of the Russian Federation work with is personal data. Because of their prevalence, they require special vigilance in their processing and security. Information systems processing personal data may be subject to various attacks due to certain vulnerabilities. To ensure maximum protection of the personal data information system, the Federal Service for Technical and Export Control has developed a special methodology for determining the current threats to the information system. In order to reduce the expert's labor in assessing each threat, the automation of this process will be relevant, which in the end will not only give a gain in time, but also reduce the number of errors associated with the human factor.
Keywords: personal data; current security threats; personal data information system; threat model; software implementation.

ВВЕДЕНИЕ

Основным объектом пристального внимания в наше время является информация. Существует множество видов информации, требующие компетентного получения, хранения, обработки и защиты. Информация о личных данных человека всегда имела и будет иметь большой спрос.

Основной проблемой является наличие персональных данных в любой организации, коммерческой или государственной. Утечка таких данных может привести к финансовым убыткам, административным или уголовным последствиям. Наряду с ростом технических возможностей для копирования и распространения информации возросла необходимость своевременного принятия мер по качественной защите персональных данных.

Уровень информационных технологий на данном этапе развития человечества довольно высок. В силу этого, самозащита информационных прав перестала функционировать эффективно. В современных реалиях человек физически не может добиться скрытности от всего изобилия применяемых в отношении него технических и программных средств и методов сбора или хищения данных, поэтому одна из самых актуальных проблем – это проблема защиты персональных данных [1].

Для построения адекватной системы защиты персональных данных на начальном этапе составляется список реальных угроз безопасности. Используя данный перечень актуальных угроз и уровень исходной защищенности, формулируются конкретные организационно-технические требования по защите информационных систем от утечки данных по техническим каналам, от несанкционированного доступа [2]. Также осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.

ОСНОВНАЯ ЧАСТЬ

Система безопасности включает в себя защиту информации только для актуальных угроз. В соответствии с пунктом 2 статьи 19ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз [3].

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, определение уровня исходной защищенности производится на основании анализа технических и эксплуатационных характеристик ИСПДн [4].

Однако данная методика реализована только на материальных носителях, что усложняет расчет и поиск актуальных угроз, что увеличивает время работы экспертов и затраты. Для исправления данного фактора разработана программная реализация методики на языке разметки HTML, то есть получить доступ к данной разработке можно при наличии интернета и веб-браузера.

Hyper Text Markup Language является стандартным языком разметки документов в глобальной сети. Его разработал британский ученый Тим Бернернс-Ли в 1990-х годах. Целью этого языка было упрощение обмена научной и технической документации [5].

HTML-страницы или гипертекстовые документы преобразуются браузером на стороне пользователя, в удобный для чтения вид. Это позволяет просматривать информацию в различных формах, например, изображения, текст, таблицы. При этом данный язык позволяет составить сложную иерархическую структуру из аналогичных документов.

При написании кода на данном языке используются специальные пометки или теги. Тегами обозначается начало и конец элемента, при этом любой документ, написанные с использованием HTML является набором таких элементов. Они могут быть пустыми, вложенными или иметь

собственные атрибуты, которые будут определять какие-либо свойства элемента. Кроме элементов существуют сущности – это специальные символы со знаком амперсанта.

Основной задачей языка является размещение элементов на странице, то есть он предназначен для создания статических веб-страниц. При этом он является самым демократичным языком, благодаря тому, что может подстроиться под каждый из браузеров [6].

На текущем этапе реализована поддержка только одного эксперта, добавление количества экспертов, разработка продукта на мобильную платформу и автоматическая генерация отчетов будет реализована в 2019 г.

При открытии страницы с реализованным расчетом актуальных угроз, эксперту предлагается определить характеристики информационной системы по таким критериям как наличие выхода в глобальную сеть интернет, территориальное размещение, разрешенные действия с данными и дальнейшие критерии, утвержденные методикой (рис. 1). Верный выбор данных свойств позволит программе определить коэффициент исходной защищенности информационной системы.

Во второй таблице эксперт оценивает вероятные угрозы системы по двум критериям: критичность и вероятность реализации.

Расчет исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению:	
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом	◉
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)	○
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	○
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий	○
локальная ИСПДн, развернутая в пределах одного здания	○
2. По наличию соединения с сетями общего пользования:	
ИСПДн, имеющая многоточечный выход в сеть общего пользования	○
ИСПДн, имеющая одноточечный выход в сеть общего пользования	○
ИСПДн, физически отделенная от сети общего пользования	○
3. По встроенным (легальным) операциям с записями баз персональных данных	
чтение, поиск	◉
запись, удаление, сортировка	○
модификация, передача	○
4.По разграничению доступа к персональным данным	
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	○
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	○
5. По наличию соединений с другими базами ПДн иных ИСПДн	
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)	○
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	○
6. По уровню обобщения (обезличивания) ПДн	
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	○
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	○
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	○
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	

Рис. 1. Таблица расчета исходной защищенности ИСПДн
Fig. 1. Table of calculation of initial security of ISPD

Предложены наиболее распространенные угрозы утечки информации, такие как акустические, видовые, побочные электромагнитные излучения (ПЭМИН), хищение средств хранения информации, а также преднамеренные и непреднамеренные угрозы. Эксперт определяет для каждой угрозы вероятность реализации, исходя из предложенных четырех вариантов и показатель опасности (предложено 3 варианта ответа) (рис. 2, 3).

После заполнения всех данных эксперту необходимо нажать кнопку «Закончить» после таблиц. Программы рассчитает угрозы по утвержденным методикой баллам и определит наиболее актуальные угрозы информационной системе персональных данных (рис. 4).

Экспертные оценки

Угрозы утечки акустической (речевой) информации	Вероятность реализации	Показатель опасности
Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.	Маловероятно	Низкий
Угрозы утечки видовой информации		
Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.	Маловероятно (Маловероятно, Низкая вероятность, Средняя вероятность, Высокая вероятность)	Низкий
Угрозы утечки информации по каналам ПЭМИН		
Кража ПЭВМ и кража носителей информации. Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.	Маловероятно	Низкий
Кража ключей и атрибутов доступа. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.	Маловероятно	Низкий
Кражи, модификации, уничтожения информации. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.	Маловероятно	Низкий
Несанкционированное отключение средств защиты. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.	Маловероятно	Низкий
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
Действия вредоносных программ (вирусов). Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программа с потенциально опасными последствиями или вредоносной программой (вирусом).	Маловероятно	Низкий
Не декларированные возможности системного ПО и ПО для обработки персональных данных. Не декларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.	Маловероятно	Низкий
Установка ПО не связанного с исполнением служебных обязанностей. Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.	Маловероятно	Низкий
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении.		
Утрата ключей и атрибутов доступа. Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают		

Рис. 2. Варианты вероятности реализации угроз
Fig. 2. Variants of the likelihood of threats

Экспертные оценки

Угрозы утечки акустической (речевой) информации	Вероятность реализации	Показатель опасности
Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.	Маловероятно	Низкий
Угрозы утечки видовой информации		
Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.	Маловероятно	Низкий
Угрозы утечки информации по каналам ПЭМИН		
Кража ПЭВМ и кража носителей информации. Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.	Маловероятно	Низкий
Кража ключей и атрибутов доступа. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.	Маловероятно	Низкий (Низкий, Средний, Высокий)
Кражи, модификации, уничтожения информации. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.	Маловероятно	
Несанкционированное отключение средств защиты. Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.	Маловероятно	Низкий
Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
Действия вредоносных программ (вирусов). Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программа с потенциально опасными последствиями или вредоносной программой (вирусом).	Маловероятно	Низкий
Не декларированные возможности системного ПО и ПО для обработки персональных данных. Не декларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.	Маловероятно	Низкий
Установка ПО не связанного с исполнением служебных обязанностей. Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.	Маловероятно	Низкий
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении.		
Утрата ключей и атрибутов доступа. Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают		

Рис. 3. Варианты показателя опасности угроз
Fig. 3. Hazard indicator variants

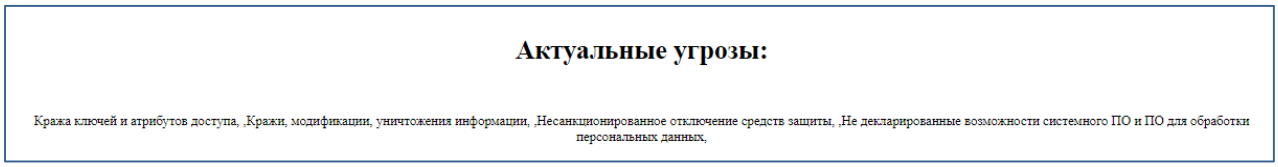

Рис. 4. Результат оценки
Fig. 4. Evaluation result

ЗАКЛЮЧЕНИЕ

Таким образом, данный метод позволит определить актуальные угрозы, имея доступ к сайту с данной формой, однако так как временно существует поддержка только одного эксперта, оценка является субъективной, то есть, возможно, потребуется оценка другого эксперта, для определения общих актуальных угроз.

Список литературы

1. Олег Слепов. Защита персональных данных // ИТ-портал компании «Инфосистемы Джет»: электронный журнал, 2009. №5. URL: http://www.jetinfo.ru/jetinfo_arhiv/zaschita-personalnykh-dannykh/zaschita-personalnykh/2017 (дата обращения: 11.12.2018).

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-телеком, 2001. 148 с.

3. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 10.12.2018).

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380/ (дата обращения: 12.11.2018).

5. HTML: основы для начинающих. URL: http://fb.ru/article/250376/html-osnovyi-dlya-nachinayuschih/ (дата обращения: 14.12.2018).

6. Что такое HTML. URL: https://blogwork.ru/chto-takoe-html/ (дата обращения: 14.12.2018).

References

1. Oleg Slepov. Protection of personal information. Jet Infosystems IT portal: electronic journal, 2009. №5. URL: http://www.jetinfo.ru/jetinfo_arhiv/zaschita-personalnykh-dannykh/zaschita-personalnykh/2017 (handling date: 11/12/2018).

2. Malyuk A.A., Pazizin S.V., Pogozhin N.S. Introduction to information security in automated systems. Moscow: Goryachaya liniya-telekom, 2001. 148.

3. Federal Law “On Personal Data” dated July 27, 2006 No. 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (handling date: 10/12/2018).

4. The method of determining the actual threats to the security of personal data during their processing in the information systems of personal data. FSTEC of Russia, 2008. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380/ (handling date: 12/11./018).

5. HTML: Basics for Beginners. URL: http://fb.ru/article/250376/html-osnovyi-dlya-nachinayuschih/ (handling date: 12/14/2018).

6. What is HTML? URL: https://blogwork.ru/chto-takoe-html/ (handling date: 12/14/2018).

Гончаренко Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры «Информационная безопасность»
Кушнарев Александр Александрович, студент первого курса магистратуры кафедры «Информационная безопасность»
Исаков Сергей Алексеевич, студент четвертого курса кафедры «Информационная безопасность»

Goncharenko Julia, Doctor of Technical Sciences, Professor of "Information security"
Kushnaryov Aleksandr, First-Year Master's Student of the Department "Information security"
Isakov Sergey, Fourth-Year Student of the Department "Information security"