РАЗРАБОТКА МОДЕЛИ УГРОЗ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Ларионов К.О.
Email: Larionov17163@scientifictext.ru

Ларионов Константин Олегович – аспирант,
кафедра вычислительной техники и защиты информации,
Оренбургский государственный университет, г. Оренбург

Аннотация: *в статье рассматривается типовая модель угроз прикладного программного обеспечения. По статистике чаще всего угрозы информационной безопасности направлены на веб-приложения. Актуальность разработки типовой модели угроз обуславливается тем, что специфика данной предметной области не позволяет разглашать частные модели угроз для прикладного программного обеспечения, а общих моделей угроз в общедоступных источниках не имеется. В большинстве случаев угрозы, реализующиеся через подмену программного обеспечения или подмену подписей, являются более актуальными.*
Ключевые слова: *программное обеспечение, модель угроз, защита программного обеспечения, система, модель, нарушитель, угроза.*

DEVELOPMENT OF THE APPLIED SOFTWARE THREAT MODEL

Larionov K.O.

Larionov Konstantin Olegovich – Postgraduate,
DEPARTMENT OF COMPUTING AND INFORMATION SECURITY,
ORENBURG STATE UNIVERSITY, ORENBURG

Abstract: *the article discusses a typical model of applied software threats. According to statistics, most often information security threats are directed at web applications. The relevance of developing a typical threat model is due to the fact that the specificity of this subject area does not allow disclosing private threat models for applied software, and there are no general threat models in public sources. In most cases, threats implemented through software substitution or signature substitution are more relevant.*
Keywords: *software, threat model, software protection, system, model, intruder, threat.*

УДК 004.056

Создание копий программных средств для изучения или несанкционированного использования является одним из наиболее широко распространенных правонарушений в сфере компьютерной информации, что предопределяет необходимость защиты программного обеспечения.

В общем случае под защитой программного обеспечения понимается комплекс мер, направленных на защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов.

При организации защиты программного обеспечения используются различные меры, такие как:

- организационные;
- правовые;
- технические.

Основная идея организационных мер защиты заключается в том, что полноценное использование программного продукта невозможно без соответствующей поддержки со стороны производителя подробной пользовательской документации, «горячей линии», системы обучения пользователей, обновление версий со скидкой и т.п.

Организационные меры защиты применяются, как правило, крупными разработчиками к достаточно большим и сложным программным продуктам.

Правовые меры защиты программного обеспечения заключаются в установлении ответственности за использование программного обеспечения с нарушением порядка, установленного действующим законодательством.

Так статья 7.12. Кодекса Российской Федерации об административных правонарушениях предусматривает административную ответственность за нарушение авторских и смежных прав, изобретательских и патентных прав. А статьей 146 Уголовного кодекса Российской Федерации за нарушение авторских и смежных прав, если это нарушение привело к причинению крупного ущерба, установлена уголовная ответственность.

Технические методы защиты программного обеспечения можно классифицировать по способу рас-

пространения защищаемого программного обеспечения и типу носителя лицензии. На рисунке 1 представлены статистические данные по угрозам на прикладное программное обеспечение за 2019 год.

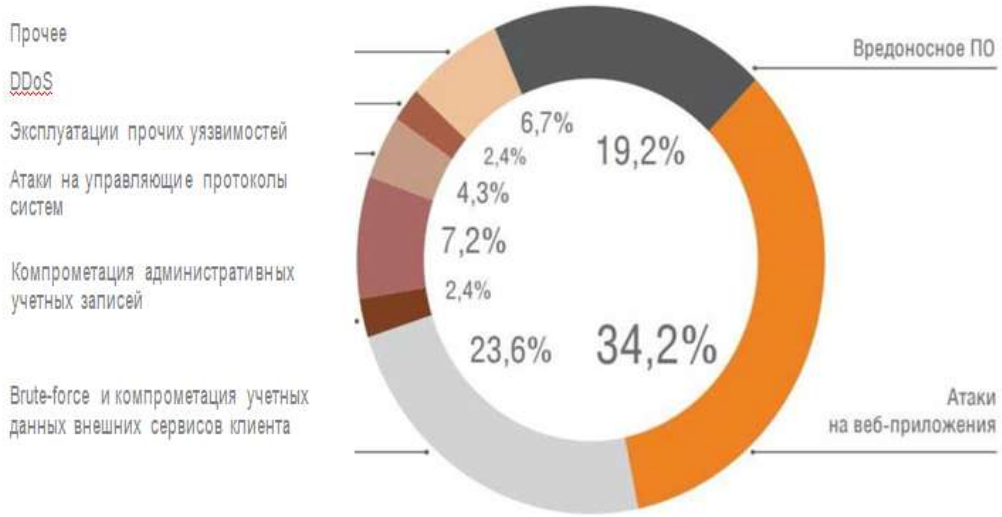

Рис. 1. Статистические данные по угрозам на прикладное программное обеспечение за 2019 год

В работе Петигина А.Ф., Мирошникова П.В. «Защита программного обеспечения базовой системы ввода-вывода в целях обеспечения доверенной загрузки» рассматриваются пути обеспечения доверенной загрузки операционной системы и средств защиты информации от несанкционированного доступа. Приводится анализ уязвимостей штатных средств обеспечения доверенной загрузки базовой системы ввода-вывода, предлагается техническое решение в сравнении с аналогами. Не рассматривается подход к построению модели угроз и модели нарушителей также не приведена классификация программного средства.

В статье Лебедева С.С. «Разработка методов и средств комплексной оценки качества систем защиты программного обеспечения» дается определение качества системы защиты программного обеспечения. Определены функции системы защиты в составе комплекса из системы защиты и защищаемого программного обеспечения. Разработана модель системы "защищаемое программное обеспечение - система защиты программного обеспечения", а также выполнен анализ работоспособности этой модели с учетом функциональных связей между ее структурными элементами.

В работе Десницкого В.А. «Модель защиты программного обеспечения на основе механизма удаленного доверия» предложен подход к построению модели защиты программ от несанкционированных изменений и вмешательств с использованием механизма "удаленного доверия". Рассмотрены основные составляющие элементы механизма и принципы его функционирования. Предложены два варианта реализации механизма замещения мобильного модуля на основе парадигмы объектно-ориентированного программирования. Однако не проведено построение общей модели угроз для программного средства.

Целью работы является снижение риска от угроз информационной безопасности в прикладном программном обеспечении.

Для достижения цели в работе поставлены следующие задачи:

1 Разработать общую классификацию программного обеспечения для выявления особенностей прикладного программного обеспечения.

Классификация программного обеспечения представлена на рисунке 2.

Рис. 2. Классификация программного обеспечения

2 Разработать типовую модель угроз для прикладного программного обеспечения:

Существующие модели угроз для автоматизированной информационной системы для прикладного программного обеспечения не удовлетворяют поставленным требованиям тем, что специфика данной предметной области не позволяет разглашать частные модели угроз для прикладного программного обеспечения, а общих моделей угроз в общедоступных источниках не имеется. Также тип моделей угроз является предполагаемым, а не расчетным или экспертным, что не дает полного понимания проблемы, так как нет базовой таблицы или базовых данных для решения актуальности конкретной угрозы.

В таблице 1 представлена типовая модель угроз для прикладного программного обеспечения.

Таблица 1. Типовая модель угроз для прикладного программного обеспечения

Номер УБИ	Наименование УБИ	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Показатель опасности угрозы	Актуальность угрозы
1	2	3	4	5	6
63	Угроза некорректного использования функционала программного и аппаратного обеспечения	Низкая	Высокая	Высокая	Актуальная
143	Угроза программного выведения из Строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Маловероятная	Низкая	Низкая	Неактуальная
145	Угроза пропуска проверки целостности программного обеспечения	Маловероятная	Низкая	Низкая	Неактуальная
162	Угроза эксплуатации цифровой подписи программного кода	Средняя	Высокая	Средняя	Актуальная
188	Угроза подмены программного обеспечения	Средняя	Высокая	Средняя	Актуальная
191	Угроза внедрения вредоносного кода в Дистрибутив программного обеспечения	Маловероятная	Средняя	Низкая	Неактуальная
192	Угроза использования уязвимых версий про-	Высокая	Средняя	Высокая	Актуальная

	граммного обеспечения				
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Средняя	Средняя	Низкая	Неактуальная
210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в *ней программного обеспечения*	Маловероятная	Маловероятная	Маловероятная	Неактуальная
217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Высокая	Высокая	Высокая	Актуальная

Таким образом, можно сделать вывод, что для типовой модели угроз прикладного программного обеспечения актуальными являются:

- угроза некорректного использования функционала программного и аппаратного обеспечения;
- угроза эксплуатации цифровой подписи программного кода;
- угроза подмены программного обеспечения;
- угроза использования уязвимых версий программного обеспечения;
- угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

Из вышеперечисленного списка актуальных угроз для данной типовой модели автоматизированной информационной системы можно выявить тенденцию, что в большинстве случаев угрозы, реализующиеся через подмену программного обеспечения или подмену подписей, являются более актуальными.

Список литературы / References

1. Угрозы информационной безопасности в 2017 году: шифровальщики, ICO, IoT-ботнеты – исследование. [Электронный ресурс]. Режим доступа: http://d-russia.ru/ugrozy-informatsionnoj-bezopasnosti-v-2017-godu-shifrovalshhiki- ico-iot-botnety-issledovanie.html/ (дата обращения: 01.11.2019).
2. Модель угроз безопасности персональных данных. [Электронный ресурс]. Режим доступа:https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/model-ugroz-bezopasnosti-personalnyh-dannyh/ (дата обращения: 01.11.2019).
3. Банк данных угроз безопасности информации [Электронный ресурс]. Режим доступ https://bdu.fstec.ru/threat/ (дата обращения: 01.11.2019).
4. *Петин А.Ф.* Защита программного обеспечения базовой системы ввода-ввывода в целях обеспечения доверенной загрузки / Петин А.Ф., Мирошников П.В. Воронеж: Издательство: Санкт-Петербургский политехнический университет Петра Великого (Санкт-Петербург), 2008. С. 101-105.
5. *Савельев И.Е.* Защита прав на программное обеспечение. Москва: Издательство: Московский университет МВД РФ им. В.Я. Кикотя (Москва), 2008. С. 88-90.
6. *Лебедев С.С.* Разработка методов и средств комплексной оценки качества систем защиты программного обеспечения. Москва: Издательство: Московский автомобильно-дорожный государственный технический университет (МАДИ) (Москва), 2007. С. 84-89.
7. *Десницкий В.А.* Модель защиты программного обеспечения на основе механизма "удаленного доверия" / Десницкий В.А., Котенко И.В. Санкт- Петербург: Издательство: Министерство науки и высшего образования РФ (Санкт-Петербург), 2008. С. 26-31.