УДК 621.396.61 DOI:10.31854/1813-324X-2021-7-2-95-101

Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения

Р.В. Жук[1]

[1]Филиал «Макрорегион Юг» ООО ИК «СИБИНТЕК»,
Краснодар, 350063, Российская Федерация
*Адрес для переписки: goonerkrd@gmail.com

Информация о статье
Поступила в редакцию 27.01.2021
Принята к публикации 22.06.2021

Ссылка для цитирования: Жук Р.В. Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. 2021. Т. 7. № 2. С. 95–101. DOI:10.31854/1813-324X-2021-7-2-95-101

Аннотация: *В настоящее время внедрено множество методических документов, регламентирующих подходы к разработке моделей угроз безопасности информации для информационных систем, обрабатывающих информацию различного характера. Существуют разные методики разработки угроз и построения модели нарушителя, предлагаемые регуляторами в области информационной безопасности, в зависимости от направления их деятельности. Для поддержки принятий решений в процессе моделирования угроз разработан банк данных угроз безопасности информации. Однако в существующих подходах имеется ряд противоречий, при этом методики определения угроз и построения модели нарушителя, в большинстве случаев, предполагают привлечение экспертов для оценки факторов и условий возникновения угроз. В существующих методиках отсутствует взаимосвязь между нарушителем безопасности информации, и уязвимостями программного обеспечения в информационных системах, что не позволяет построить адекватную модель угроз без привлечения квалифицированных экспертов. Целью данной работы является определение потенциала нарушителя безопасности информации в зависимости от его возможностей и оценка влияния данного потенциала на реализацию уязвимостей программного обеспечения в информационных системах.*

Ключевые слова: *потенциал, нарушитель безопасности информации, возможность, уязвимость, программное обеспечение, несанкционированный доступ.*

Введение

Основополагающим этапом при проектировании подсистемы защиты информации является разработка модели угроз безопасности информации, которая должна включать в себя модель нарушителя безопасности информации (далее – нарушитель). В общем случае, механизм определения угроз, представленный в [1–4], состоит из следующих этапов:

– определение и подготовка перечня источников угроз, включая нарушителей, оценку их возможностей и потенциала;

– подготовка перечня уязвимостей программного обеспечения информационной системы и ее активов для последующего анализа;

– определение способов (сценариев) реализации угроз;

– оценка последствий от реализации угроз и степень влияния выбранных угроз на свойства безопасности информации, обрабатываемой в информационной системе.

Несмотря на различное количество нарушителей, представленное в методических документах регуляторов в области информационной безопасности и защиты информации, их категорирование осуществляется с использованием мотивации, целей и типов, зависящих от наличия физического доступа внутрь контролируемой зоны, в которой размещены информационные системы. При этом, перечисленные в [5–7] нарушители обладают различными возможностями и потенциалом.

Наряду с этим, выбор способов (сценариев) реализации угроз нарушителем необходимо осуществлять с использованием банка угроз безопасности информации, что способствует подготовке перечня угроз с использованием типа и потенциа-

ла нарушителя, а также выбранных экспертным путем последствий реализации угрозы. При этом один из ключевых этапов процесса определения угроз безопасности информации, связанный с подготовкой перечня уязвимостей программного обеспечения, исключается. Дополнительно, нерешенной проблемой является отсутствие параметра потенциала для нарушителей, представленных в [5]. Таким образом, целью исследования является разработка способа установления потенциала нарушителей на основании их категорирования и подготовка алгоритма оценки влияния выбранных нарушителей на уязвимости программного обеспечения в информационной системе.

Анализ способов разработки моделей нарушителя и его влияния на угрозы безопасности информации

Впервые категорирование нарушителей по типам и возможностям было приведено в [5], однако в рамках предметной области приведенные характеристики нарушителя никак не связаны с процессом определения угроз безопасности информации. В [6] к возможностям нарушителей была добавлена мотивация (возможные цели), а также каждому нарушителю был присвоен потенциал, который позволяет для определения перечня угроз применять соответствующий банк угроз безопасности информации. Основным нововведением предлагаемого в [6] подхода является смена параметра вероятности возникновения угрозы на потенциал нарушителя при определении возможности реализации угрозы. При этом сама оценка возможности реализации угрозы представлена в виде таблицы с качественными значениями. Дополнительно, в [6] приводится способ определения потенциала нарушителя при использовании угроз безопасности информации, данные по которым не приведены в банке угроз безопасности информации. Данный способ предполагает экспертную оценку следующих возможностей на этапах идентификации и эксплуатации уязвимостей программного обеспечения: затрачиваемое время; техническая компетентность; знание проекта и возможность доступа к информационной системе; оснащенность нарушителя.

В [7] перечень видов нарушителей с присвоением потенциала представлен в зависимости от их возможностей по реализации угроз. Одной из характеристик угрозы является наличие хотя бы одного сценария ее реализации нарушителем с заданным потенциалом. Сценарий реализации угроз определяется, как совокупность тактик и техник, которые могут применяться нарушителем. Однако взаимосвязь между потенциалом и возможностями нарушителя с представленными в [7] тактиками является косвенной и должна быть установлена экспертным путем.

Дополнительно, при проектировании защиты информационных систем персональных данных (ИСПДн) необходимо руководствоваться методикой [8], которая заключается в дополнении функционала нарушителя возможностями, направленными на реализацию угроз, связанных с функционированием средств криптографической защиты информации.

В каждом из вышеперечисленных документов модель нарушителя является абстрактным понятием и может применяться справочно экспертами в ходе разработки модели угроз безопасности информации.

Наряду с регуляторами процесс построения модели нарушителя широко обсуждается в научных кругах. В 2017 г. С.О. Савченко и Н.В. Капчук в своей статье [9] изложили подход к построению модели нарушителя с использованием соотношения стратегий защитника, направленных на нейтрализацию стратегий нарушителя, реализующих множества угроз. В предлагаемом подходе для построения модели нарушителя и выбора стратегий оппонентов необходимо провести анализ рисков, ранжирование угроз безопасности информации, классифицировать систему и средства защиты; при этом механизмы и методы, которыми необходимо для этого руководствоваться, не приведены.

Ранее, в 2012 г. В.Г. Жуков, М.Н. Жукова и А.П. Стефаров в своей статье [10] предложили дополнить модели нарушителя уровнями несанкционированного доступа (НСД) к защищаемой информации в информационной системе. Классификация уровней была проведена с использованием сетевой модели TCP/IP. Однако для определения актуальности каждой угрозе и каждому нарушителю экспертным путем необходимо присвоить уровень НСД.

В работе [11] Е.А. Максимовой предложено использовать пятиуровневую модель доступа нарушителя к информации и компонентам объектов критической информационной инфраструктуры. Основными параметрами нарушителя при этом являются: возможность физического доступа; возможность логического доступа; компетенция; оснащенность; мотивация. При этом возможности физического и логического доступа, а также мотивацию предложено относить к базовому потенциалу, а оснащенность и компетенцию оценить экспертным путем с использованием качественной и количественной шкал.

Рассмотренные методы и подходы к разработке модели нарушителя, несмотря на свою значимость, не в полной мере описывают механизм оценки возможности использования им уязвимостей программного обеспечения информационной системы. В представленных работах и методиках отсутствует простой и удобной механизм выбора.

Также в них отсутствует определенный перечень нарушителей, а оценка потенциала нарушителей представлена крайне субъективно. Рассмотрим в этом контексте выбор нарушителей на примере ИСПДн.

Определение потенциала нарушителей безопасности информации

На первом этапе, согласно [5], необходимо присвоить потенциал нарушителям. Для этого воспользуемся методом анализа иерархий [12] Т. Саати. Оценка влияния критериев матрицы отношений будет осуществляться экспертным путем с использованием шкалы отношений, представленной в таблице 1.

ТАБЛИЦА 1. Шкала отношений

TABLE 1. Relationship Scale

Степень важности	Значимость
1	Одинаковая
3	Слабая
5	Сильная
7	Очень сильная
9	Абсолютная
2, 4, 6, 8	Промежуточные значения между соседними значениями шкалы

Согласно методологии Т. Саати, необходимо построить иерархические модели для трех категорий нарушителей безопасности информации – внешний, внутренний и внутренний со специальными возможностями.

Пример иерархической модели для внешнего нарушителя представлен на рисунке 1, где: НСД-I – НСД через автоматизированные рабочие места в сетях общего пользования; НСД-II – НСД с использованием специального программного обеспечения и вирусов; НСД-III – НСД через компоненты за пределами контролируемой зоны; НСД-IV – НСД через смежные информационные системы.

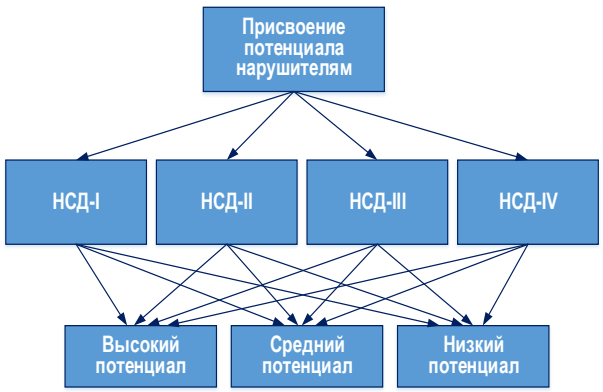

Рис. 1. Иерархическая модель определения потенциала внешнего нарушителя безопасности информации

Fig. 1. Hierarchical Model for Determining the Potential of an External Information Security Intruder

Частично матрицы отношений возможностей нарушителей к потенциалу заполняются экспертным путем с применением значений из таблицы 1. Остальные значения критериев заполняются с использованием следующей формулы:

$$x_{nm} = \frac{1}{x_{nm}}, \quad (1)$$

где x_{nm} – элемент в строке n столбца m.

Аналогичные матрицы разрабатываются для существующих альтернатив. На следующем этапе осуществляется нормирование составленных матриц по формуле:

$$X_{ij} = \frac{x_{nj}}{S_j}, \quad (2)$$

где X_{ij} – элемент i-й строки j-го столбца нормированной матрицы отношений; x_{nj} – элемент n-й строки j-го столбца матрицы отношений; S_j – сумма элементов x в j-м столбце.

Для каждой нормированной матрицы рассчитывается вес в долях по формуле:

$$D = \frac{\sum_j^1 x_i}{j}, \quad (3)$$

где x_i – элемент j-го столбца.

Примеры нормированных матриц для критериев и альтернатив потенциала нарушителей безопасности информации представлены в таблицах 2 и 3.

ТАБЛИЦА 2. Попарное сравнение критериев возможностей нарушителей

TABLE 2. Pairwise Comparison of Intruder's Capability Criteria

	НСД-I	НСД-II	НСД-III	НСД-IV	Вес в долях
НСД-I	1	0,2	3	4	0,30
НСД-II	5	1	7	0,33	0,49
НСД-III	0,33	0,14	1	0,2	0,06
НСД-IV	0,25	0,25	2	1	0,13

ТАБЛИЦА 3. Попарное сравнение альтернатив по критерию

TABLE 3. Pairwise Comparison of Alternatives by Criterion

НСД-I	Низкий	Средний	Высокий	Вес в долях
Низкий	0,13	0,14	0,10	0,12
Средний	0,50	0,57	0,60	0,56
Высокий	0,38	0,29	0,30	0,32

Аналогичные таблицы строятся для каждого оставшегося критерия (возможности нарушителя).

Потенциал нарушителя предлагается присваивать в зависимости от полученного результата при вычислении весов альтернатив по формуле:

$$A = (z_{ij}) * (y_j), \quad (4)$$

где z_{ij} – вес в долях альтернатив для каждого критерия (на примере таблицы 3); y_i – вес в долях для критериев.

Рассчитаем потенциал нарушителя на примере данных таблицы 2:

$$A = \begin{pmatrix} 0{,}12 & 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}56 & 0{,}57 & 0{,}57 & 0{,}57 \\ 0{,}32 & 0{,}33 & 0{,}33 & 0{,}33 \end{pmatrix} * \begin{pmatrix} 0{,}31 \\ 0{,}49 \\ 0{,}06 \\ 0{,}13 \end{pmatrix} = \quad (5)$$
$$= \begin{pmatrix} 0{,}11 \\ 0{,}56 \\ 0{,}33 \end{pmatrix}.$$

Видно, что перечисленным в [5] внешним нарушителям с весовой долей 0,56, вычисленной по формуле (5), может быть присвоен средний потенциал (см. таблицу 3).

По результатам использования метода при минимальном участии эксперта потенциал может быть присвоен любому нарушителю в зависимости от его возможностей.

Однако потенциала нарушителя недостаточно для определения перечня угроз безопасности информации, т. к. другим не менее значимым фактором угрозы НСД является наличие уязвимости программного обеспечения. При использовании возможностей или потенциала нарушителей для подготовки перечня таких уязвимостей, которые позволят реализовать угрозы НСД в рассматриваемой ИСПДн, возникает необходимость привлечения экспертов. Сам процесс выбора и сопоставления уязвимостей и нарушителей в информационных системах не регламентирован.

Для организации взаимосвязи уязвимостей программного обеспечения и потенциала нарушителя информационной безопасности рекомендуется спроецировать базовые метрики вектора уязвимости программного обеспечения на возможности потенциала нарушителя. При этом для описания потенциала нарушителя предлагается использовать унифицированные возможности, аналогично приведенным в [11], которые могут быть спроецированы на метрики уязвимостей с использованием метода из [12]:

– техническая компетентность;

– знание проекта и информационной системы;

– возможность доступа к информационной системе;

– оснащенность нарушителя.

Иерархическая модель проецирования метрик вектора уязвимости программного обеспечения на возможности нарушителя представлена на рисунке 2.

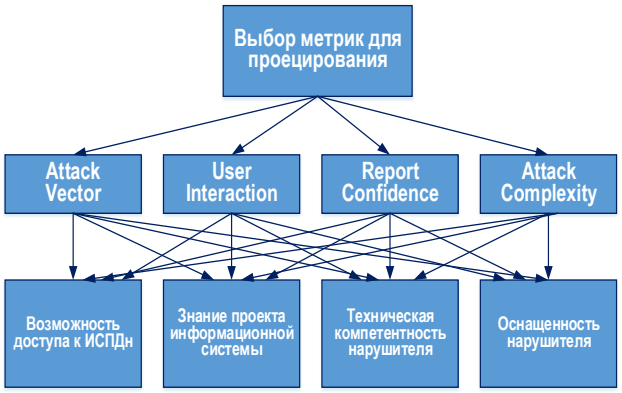

Рис. 2. Иерархическая модель проецирования метрики вектора уязвимости программного обеспечения на возможности потенциала нарушителя

Fig. 2. Hierarchical Model of Projection of the Vulnerability Metric of the Security Potential of the Attacker

Количественные значения параметрам данных метрик присваиваются с применением градации [13] и далее могут выступать, как условие возможности использования существующего в информационной системе уязвимости программного обеспечения выбранным ранее нарушителем с установленным потенциалом (таблица 4).

ТАБЛИЦА 4. Проецирование параметров вектора уязвимостей на возможности потенциала нарушителя

TABLE 4. Projecting the Parameters of the Vulnerability Vector onto the Capabilities of the Intruder's Potential

Метрика уязвимости программного обеспечения	Возможности нарушителя	Наибольший весовой коэффициент
Attack Vector (AV)	Возможность доступа к ИСПДн	0,52
User Interaction (UI)	Знание проекта информационной системы	0,41
Report Confidence (RC)	Техническая компетентность	0,32
Attack Complexity (AC)	Оснащенность	0,53

Таким образом, спроецированным значениям нарушителя экспертным путем могут быть присвоены количественные значения из верхнего диапазона, представленного в [13]. Для оценки возможности использования уязвимости программного обеспечения нарушителями с заданным потенциалам может быть разработана продукционная модель прямого вывода [14], состоящая из следующих правил:

– *реализуемая уязвимость*: если «AV уязвимости актива» <= «AV нарушителя» и «UI уязвимости актива» <= «UI нарушителя» и «RC уязвимости актива» <= «RC нарушителя» и «AC уязвимости актива» <= «AC нарушителя», то «Уязвимость №» = «Актуальная уязвимость»;

– *нереализуемая уязвимость*: если «AV уязвимости актива» > «AV нарушителя» или «UI уязвимости актива» > «UI нарушителя» или «RC уязвимо-

сти актива» > «RC нарушителя» или «AC уязвимости актива» > «AC нарушителя», то «Уязвимость №» = «Не Актуальная уязвимость».

На основании вышеперечисленных правил может быть построен алгоритм определения возможности реализации уязвимости программного обеспечения нарушителем с заданным потенциалом (рисунок 3).

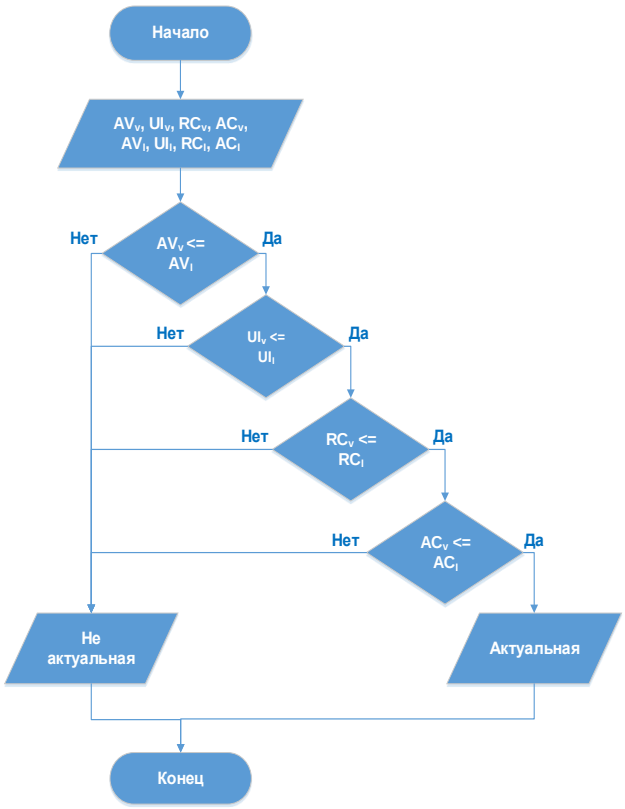

Рис. 3. Блок-схема алгоритма

Fig. 3. Flowchart of the Algorithm

Работа алгоритма состоит в следующем. На вход, с одной стороны, подаются количественные значения базовых метрик вектора уязвимостей программного обеспечения, перечень которых подготовлен на этапе определения активов информационной системы. С другой стороны, заранее определенные экспертным путем количественные значения возможностей нарушителя. Далее, по представленным выше правилам осуществляется попарное сравнение количественных значений базовых метрик вектора уязвимостей программного обеспечения информационной системы и возможностей нарушителя (см. таблицу 4). При положительном исходе, в результате выполнения всех приведенных в алгоритме условий, уязвимость программного обеспечения признается возможной к использованию выбранным нарушителем (т. е. актуальной); при невыполнении хотя бы одного из установленных условий – неактуальной.

Заключение

Предлагаемый способ определения потенциала нарушителя и реализуемых им уязвимостей программного обеспечения может применяться независимо от вида информационной системы и информации, обрабатываемой в ней. Основным преимуществом предлагаемого способа является возможность динамического и своевременного внесения изменений в модель угроз безопасности информации и переоценке возможностей нарушителя, что обеспечивается использованием комбинации удачно выбранного классического метода экспертной оценки и оригинального авторского алгоритма.

Использование метода анализа иерархий для установления потенциала нарушителей, а также при проецировании потенциала на параметры вектора уязвимости программного обеспечения, является простым и понятным инструментом, которым дополнительно могут руководствоваться эксперты при разработке моделей угроз безопасности для информационных систем, обрабатывающих информацию различного характера.

Данный метод позволяет исключить сложные вычислительные операции и сократить временные затраты экспертов, при этом позволяет подготовить исчерпывающий перечень уязвимостей программного обеспечения, которые могут быть реализованы выбранными нарушителями с заданным потенциалом.

Использование алгоритма определения возможности реализации уязвимости программного обеспечения информационной системы нарушителем с заданным потенциалом позволяет организовать взаимосвязь между его возможностями и характеристиками уязвимости. Основное достоинство данного алгоритма заключается в организации попарного сравнения количественных значений уязвимостей программного обеспечения, заранее установленных банком угроз безопасности информации, и установленных экспертным путем количественных значений возможностей нарушителя, что упрощает процесс подготовки перечня актуальных уязвимостей программного обеспечения в информационной системе.

Предлагаемый способ может быть дополнен путем построения взаимосвязи между уязвимостями программного обеспечения и угрозами безопасности информации, представленными в банке угроз безопасности информации.

Список используемых источников

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
2. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
3. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Базовая модель угроз персональных данных при их обработке в информационных системах персональных данных. Москва, 2008. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения 06.01.2021)
6. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» URL: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/114-tekhnicheskaya-zashchita-informatsii/dokumenty/spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения 06.01.2021)
7. Методический документ ФСТЭК России «Методика моделирования угроз безопасности информации». URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty/2070-metodicheskij-dokument (дата обращения 06.01.2021)
8. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России № 149/7/2/6-432 от 31.03.2015.
9. Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр // Динамика систем, механизмов и машин. 2017. Т. 5. № 4. С. 84–89. DOI:10.25206/2310-9793-2017-5-4-84-89
10. Жуков В.Г., Жукова М.Н., Стефаров А.П. Модель нарушителя прав доступа в автоматизированной системе // Программные продукты и системы. 2012. № 2. С. 75–78.
11. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91–103. DOI:10.31854/1813-324X-2020-6-4-91-103.
12. Саати Т. Принятие решений. Метод анализа иерархий. Пер. с англ. М.: Радио и связь, 1993. 278 с.
13. Калькулятор метрик уязвимостей. URL: https://www.first.org/cvss/calculator/cvsscalc30.js, (дата обращения: 08.01.2020)
14. Хомоненко А.Д., Бубнов В.П., Басыров А.Г. Модели и методы исследования информационных систем. Монография. СПб.: Изд-во Лань, 2019. 204 с.

* * *

Method for Determining the Potential of an Information Security Intruder and Realizable Software Vulnerabilities

R. Zhuk[1]

[1]Branch "Macroregion Yug" LLC IC "SIBINTEK",
Krasnodar, 350063, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-2-95-101
Received 27th January 2021
Accepted 22nd June 2021

For citation: Zhuk R. A Method for Determining the Potential of an Information Security Intruder and Realizable Software Vulnerabilities. *Proc. of Telecom. Universities.* 2021;7(2):95–101. (in Russ.) DOI:10.31854/1813-324X-2021-7-2-95-101

Abstract: *Currently, many methodological documents have been developed that regulate approaches to the development of models of threats to information security. for information systems that process information of a different nature. There are different methods of threat development and intruder model building proposed by information security regulators, depending on the direction of their activity. To support decision-making in the process of threat modeling, a databank of information security threats has been developed. However, there are a number of contradictions in existing approaches, while the methods for identifying threats and building a model of an intruder, in most cases, involve the involvement of experts to assess the factors and conditions for the emergence of threats. In the existing methods, there is no relationship between the violator of information security. and software vulnerabilities in information systems, which does not allow building an adequate threat model without the involvement of qualified experts. The purpose of this work is to determine the potential of an information security violator. depending on its capabilities and assessing the impact of this potential on the implementation of software vulnerabilities in information systems.*

Keywords: *potential, information security intruder, opportunity, vulnerability, software, unauthorized access.*

References

1. Federal Law No. 152-FZ of 27.07.2006 "On Personal Data". (in Russ.)
2. Order of the Federal Service for Technical and Export Control of Russia No. 17 of 11.02.2013 "On Approval of Requirements for the Protection of Information that Does Not Constitute a State Secret Contained in State Information Systems" (in Russ.)
3. Order of the Federal Service for Technical and Export Control of Russia No. 31 of 14.03.2014 "On Approval of Requirements for Ensuring the Protection of information in automated control systems for Production and Technological Processes at Critical Facilities, Potentially Dangerous Facilities, as well as Objects that pose an Increased danger to Human Life and health and to the environment" (in Russ.)
4. Order of the Federal Service for Technical and Export Control of Russia № 21 of 18.02.2013 "On Approval of Composition and Content of Organizational and Technical Measures for Ensuring Personal Data Security During their Processing in Personal Data Information Systems" (in Russ.)
5. *The Basic Model of Threats to Personal Data During their Processing in Personal Data Information Systems*. Moscow, 2008. Available from: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god [Accessed 6th January 2021] (in Russ.)
6. Methodological document of the Federal Service for Technical and Export Control of Russia "Methodology for Determining Information Security Threats in Information Systems". Available from: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/114-tekhnicheskaya-zashchita-informatsii/dokumenty/spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god [Accessed 6th January 2021] (in Russ.)
7. Methodological document of the Federal Service for Technical and Export Control of Russia "Methodology for Modeling Information Security Threats" Available from: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty/2070-metodicheskij-dokument [Accessed 6th January 2021] (in Russ.)
8. Methodological Recommendations for the Development of Regulatory Legal Acts Defining Threats to the Security of Personal Data that are Relevant in the Processing of Personal Data in Personal Data Information Systems Operated in the Implementation of Relevant Activities. No. 149/7/2/6-432 of 31.03.2015 (in Russ.)
9. Savchenko S.O., Kapchuk N.V. Algorithm for Constructing the Intruder Model in the Information Security System Using Game Theory. *Dynamics of Systems, Mechanisms and Machines*. 2017;5(4):84–89 (in Russ.). DOI:10.25206/2310-9793-2017-5-4-84-89
10. Zhukov V.G., Zhukova M.N., Stefarov A.P. Model of an Access Rights Intruder in an Automated System. *Programmnye produkty i sistemy*. 2012;2:75–78 (in Russ.)
11. Maximova E. Cognitive Modeling of Destructive Malicious Impacts on Critical Information Infrastructure Objects. *Proc. of Telecom. Universities.* 2020;6(4):91–103 (in Russ.) DOI:10.31854/1813-324X-2020-6-4-91-103
12. Saati T. *Decision Making. Hierarchy Analysis Method*. Translated from English. Moscow: Radio i sviaz Publ.; 1993. 278 p. (in Russ.)
13. Vulnerability Metrics Calculator. URL: https://www.first.org/cvss/calculator/cvsscalc30.js (Accessed 8 January 2020)
14. Khomonenko A.D., Bubnov V.P., Basyrov A.G. *Models and Research Methods for Information Systems*. St. Petersburg: Lan Publishing House; 2019. 204 p. (in Russ.)

Сведения об авторе:

ЖУК Роман Владимирович
начальник отдела информационной безопасности филиала «Макрорегион Юг» ООО ИК «СИБИНТЕК», goonerkrd@gmail.com
https://orcid.org/0000-0002-6604-9443