Ольга С. Макарова[1], Сергей В. Поршнев[1,2]
[1]Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, ул. Мира, 19, Екатеринбург, 620002, Россия
[2]Институт математики и механики Уральского отделения Российской академии наук, ул. Софьи Ковалевской, 16, Екатеринбург, 620108, Россия
[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702
[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ, ВЛИЯЮЩИХ НА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ НАРУШИТЕЛЕМ

DOI: http://dx.doi.org/10.26583/bit.2021.2.01

Аннотация. Одной из актуальных задач информационной безопасности (ИБ) является прогнозирование вероятностей угроз ИБ для организации, реализуемых из-за компьютерной атаки (КА). Существующие методологии по оценке компьютерных атак (КА) Cyber Kill Chain, Mitre Att&ck, NIST 800-115, Certified Ethical Hacker (CEH), ФСТЭК России и ISO 27001 предлагают подходы к анализу КА с точки зрения организации. В статье предложен совершенно новый подход по прогнозированию КА с точки зрения нарушителя. Проведен анализ КА с точки зрения нарушителя. Выделены методов КА, обсуждаемых нарушителями в сети DarkNet, и их структуризация. Обоснованы этапы реализации КА с точки зрения нарушителя: теоретическая подготовка, практическая подготовка, достижение цели КА. Обоснован вывод о возможности использования математического аппарата клеточных автоматов при моделировании КА, так как динамика КА подобна динамике клеточного автомата. Определены параметры, влияющие на возможность реализации КА нарушителем, в частности, известность метода КА, наличие/достаточность средств защиты от данной КА и другие. Обоснованы количественные характеристики КА, определяющие весовым коэффициентом перехода (ВКП). Достаточность перечня выбранных количественных характеристик КА подтверждается результатами анализа КА, реализованной с помощью вредоносного программного обеспечения Petya, на узлы информационной инфраструктуры организаций, находящихся на территории Украины.
Ключевые слова: прогнозирование, компьютерные атаки, нарушитель, весовой коэффициент перехода, теория клеточный автомат.
Для цитирования: МАКАРОВА, Ольга С.; ПОРШНЕВ, Сергей В. ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ, ВЛИЯЮЩИХ НА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ НАРУШИТЕЛЕМ. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 06–20, 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1336>. Дата доступа: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

Благодарности. Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ).

Olga S. Makarova[1], Sergey V. Porshnev[1,2]
[1]Ural Federal University,
19 Mira str., Ekaterinburg, 620002, Russia
[2]Institute of mathematics and mechanics of the Ural branch of the Russian Academy of Sciences,
Sophia Kovalevskaya str., 16, Ekaterinburg, 620108, Russia
[1]e-mail: o.s.makarova@urfu.ru, https://orcid.org/0000-0003-4585-6702
[2]e-mail: s.v.porshnev@urfu.ru, https://orcid.org/0000-0001-8620-0350

Determination of parameters affecting the possibility of computer attack implemented by an intruder

DOI: http://dx.doi.org/10.26583/bit.2021.2.01

Abstract. One of the urgent tasks of information security (IS) is to predict the probabilities of IS threats to an organization that are implemented due to a computer attack (CA). Existing methodologies for assessing CA are Cyber Kill Chain, Mitre Att&ck, NIST 800-115, Certified Ethical Hacker (CEH), FSTEC of Russia and ISO 27001/ They offer approaches to the analysis of CA from the organization point of view. The article offers a completely new approach to CA predicting from the intruder point of view. The analysis of the CA from the intruder point of view is carried out. The methods of CA discussed by intruder s in the DarkNet and their structuring are highlighted. The stages of the implementation of the SC from the intruder point of view are justified: theoretical training, practical training, achieving the goal of the CA. The conclusion about the possibility of using the mathematical apparatus of cellular automata in the simulation of the CA is justified, since the dynamics of the CA is similar to the dynamics of a cellular automaton. The parameters that affect the possibility of implementing the CA by the intruder are determined, in particular, the popularity of the CA method, the availability/sufficiency of means of protection against this CA, and others. The quantitative characteristics of the CA that determine the weighting factor of the transition (WCP) are justified. The sufficiency of the list of selected quantitative characteristics of the CA is confirmed by the results of the analysis of the CA, implemented with the help of the malicious software Petya, on the nodes of the information infrastructure of organizations located on the territory of Ukraine.

Keyword: prediction, computer attacks, intruder, weighting factor of the transition, theory of cellular automata.

For citation: MAKAROVA, Olga S.; PORSHNEV, Sergey V. Determination of parameters affecting the possibility of computer attack implemented by an intruder. IT Security (Russia), [S.l.], v. 28, n. 2, p. 06–20, 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1336>. Date accessed: 09 apr. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.01.

Acknowledgement. The reported study was funded by Russian Ministry of Science (information security).

Введение

В [1–3] предложена научно обоснованная методика оценки вероятности компьютерной атаки (КА), в которой ключевые факторы КА выбираются на основе теории положений по криминологии, разработанной Ч. Беккариа и И. Бентамом [4–6], в соответствии с которой нарушитель реализует КА при условии достаточности ожидаемой выгоды от КА и наличия возможности ее реализации, поэтому вероятность реализации КА $p(EU)$ равняется отношению условной вероятности достаточности ожидаемой полезности от КА $p(EU/A)$ к вероятности наличия возможности реализации КА нарушителем $p(A)$:

$$p(EU) = \frac{p(EU/A)}{p(A)}. \quad (1)$$

При этом в (1) $p(EU/A)$ и $p(A)$ зависят от ключевых факторов КА.

Ключевые факторы КА определены и обоснованы в [1]:

1) выгода атакующего в случае успешной реализации атаки (при оценке по данному показателю подразумевалось, что нарушитель преимущественно стремится использовать те типы атак, инциденты по которым либо не расследуются, либо в ходе расследования нарушителя не удается обнаружить и привлечь к ответственности);

2) защита от преследования (при оценке по данному показателю подразумевалось, что нарушитель преимущественно стремится использовать такие типы атак, инциденты по которым либо не расследуются, либо в ходе расследования нарушителя не удается обнаружить и привлечь к ответственности);

3) длительность атаки (при оценке по данному показателю следует выбирать наиболее быструю атаку, напомним, что по данным Лаборатории Касперского средняя продолжительность целевой атаки составляет 100 дней [7]);

4) доступность методов для реализации атаки (при оценке по данному показателю будем оценивать доступность и известность технологии реализации атаки, наличие инструментов для реализации атаки в свободном доступе, а также активное обсуждение («объяснение») атаки на форумах DarkNet [8]).

Для удобства дальнейшего анализа и использования сгруппируем ключевые факторы в два укрупненных фактора КА:

– фактор «Возможность атаки» (критерии выбора объекта КА нарушителем, этапы и методы реализации КА, методы получения информации об объекте КА, критерии выбора объекта КА нарушителем, навыки нарушителя, длительность атаки);

– фактор «Ожидаемая полезность» (включает в себя мотивы нарушителя, принципы принятие решения о проведении/продолжении/прекращении КА нарушителем).

Анализ укрупненного фактора «Ожидаемая полезность» проведен в [3], где обосновано, что количество КА за определенный период времени зависит от вероятности того, что КА не будет своевременно обнаружена, тяжести наказания, наличия и величины альтернативных доходов (выгод) у нарушителя.

Отдельно отметим, что в [1] приведен анализ существующих подходов к анализу и прогнозированию компьютерных атак, в результате которого было выявлено, что классические подходы:

– рассматривают вероятность реализации КА с точки зрения тяжести последствий для организации;

– при оценке вероятности КА не учитывается динамика;

– определяют ограниченный набор вариантов возможных векторов КА при построении системы защиты информационной безопасности.

В данной статье приведено обоснование и анализ параметров, входящих в укрупненный фактор «Возможность атаки», для обоснования которой проводится анализ существующих моделей угроз ИБ и КА: Cyber Kill Chain [9, 10], Mitre Att&ck [11], NIST 800-115 [12], Certified Ethical Hacker (CEH) [13], методология ФСТЭК России [14, 15] и методологии ISO 27001 [16].

1. Анализ методов компьютерных атак

База Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge) была создана в 2013 г. для «составления структурированной матрицы используемых киберпреступниками приемов, чтобы упростить задачу реагирования на киберинциденты» [11]. Она содержит структурированный список тактик, техник и общеизвестных фактов о нарушителях, разделенный на группы в зависимости от этапа и цели использования, представленный в виде матрицы. Классификация методов, размещенных в базе Mitre Att&ck проведена на основе задачи, реализуемой нарушителем на объект КА, список которых содержит:

– получение первоначального доступа (Initial Access);
– выполнение (Execution);
– закрепление (Persistence);
– повышение привилегий (Privilege Escalation);
– обход защиты (Defense Evasion);
– получение учетных данных (Credential Access);

– обнаружение (Discovery);
– боковое перемещение (Lateral Movement);
– сбор данных (Collection);
– эксфильтрация или утечка данных (Exfiltration);
– командование и управление (Command and Control);
– влияние (Impact).

Напомним, что в методологии ФСТЭК России [14] под понятием «угроза безопасности информации (БИ)» подразумевается «совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа» к информации. Результатом такого доступа могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке информации в информационной системе. При этом, априори, полагается, что каждая из угроз формируется взаимосвязью источников угроз, способов реализации угроз, уязвимостей и последствий [14, 15]. Структурная схема канала реализации угрозы БИ приведена на рис. 1.

Рис. 1. Структурная схема канала реализации угрозы
Fig. 1. Structural diagram of the threat implementation channel

При формировании перечня угроз БИ необходимо использовать банк данных угроз ФСТЭК России (более 200 угроз) [17], который в терминах Mitre Att&ck [9] представляет собой перечень возможных уязвимостей объектов КА (содержит информацию о более чем 27 тыс. уязвимостей) и методов реализации КА. Сама методология ФСТЭК России [14] позволяет сформировать полный перечень угроз (методов КА) и выполнить их классификацию по следующим признакам канала реализации угроз БИ:

– по виду защищаемой информации;
– по видам возможных источников;
– по способу реализации угрозы БИ;
– по виду нарушаемого свойства информации;
– по используемой уязвимости;
– по объекту воздействия.

Отметим, что помимо формирования перечня угроз БИ особое внимание необходимо также уделять оценке опасности реализации данной угрозы ИБ. Опасность реализации угрозы определяется, например, степенью негативных последствий для субъектов персональных данных (ПД). Действительно, любая система защиты информации, в том числе, предназначенная для обнаружения нарушителей, в первую очередь, нацелена на выявление действий, направленных против защищаемой информации, в частности, ПД. При этом в соответствие с методологией ISO 27001 [16] риски безопасности информации, меньшие некоторого приемлемого уровня, считаются приемлемыми. Такой уровень может быть у активов с низкой ценностью для организации. В результате КА на информационные ресурсы, не относящиеся к ценным активам для данной организации, может пройти незамеченной. Анализ фиксации обращений в правоохранительные органы по факту киберпреступлений показывает, что они происходят только в случае нарушения свойств критичной (защищаемой) организацией

информации. Краткий обзор тем активно обсуждаемых на форумах и чатах DarkNet [1–3, 18] можно поделить на следующие категории:

– продажа вредоносного программного обеспечения (ВПО);
– продажа эксплойтов;
– продажа данных;
– продажа доступов, т.е. сведений, с помощью которых можно осуществить несанкционированный доступ к сайту или серверу с последующей возможностью загрузки файлов или выполнения команд;
– продажа услуг.

Стоимость различного ПО и услуг в DarkNet варьируется от 1$ до 2540 $. На рис. 2 приведено процентное соотношение упоминаний о различных методах и инструментах реализации КА.

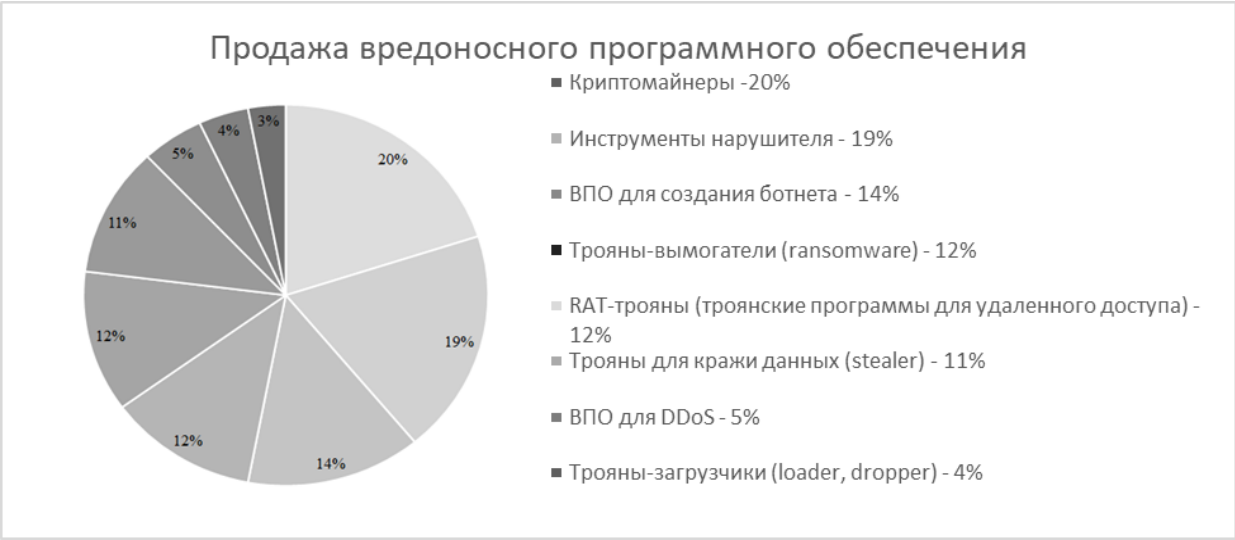

Рис. 2. Процентное соотношение продаваемых методов и инструментов для реализации КА в DarkNet
Fig. 2. Percentage of sold methods and tools for the implementation of CA in DarkNet

На рис. 3 приведено процентное соотношение данных о продаже различных услуг для реализации КА.

Анализ полученных данных позволяет сделать вывод, что выбор конкретного метода проведения КА определяется:

– наличием и известностью метода КА, в том числе в DarkNet;
– отсутствием мер защиты от КА;
– не реализуются мероприятия по мониторингу КА;
– отсутствием видимого вреда для объекта КА.

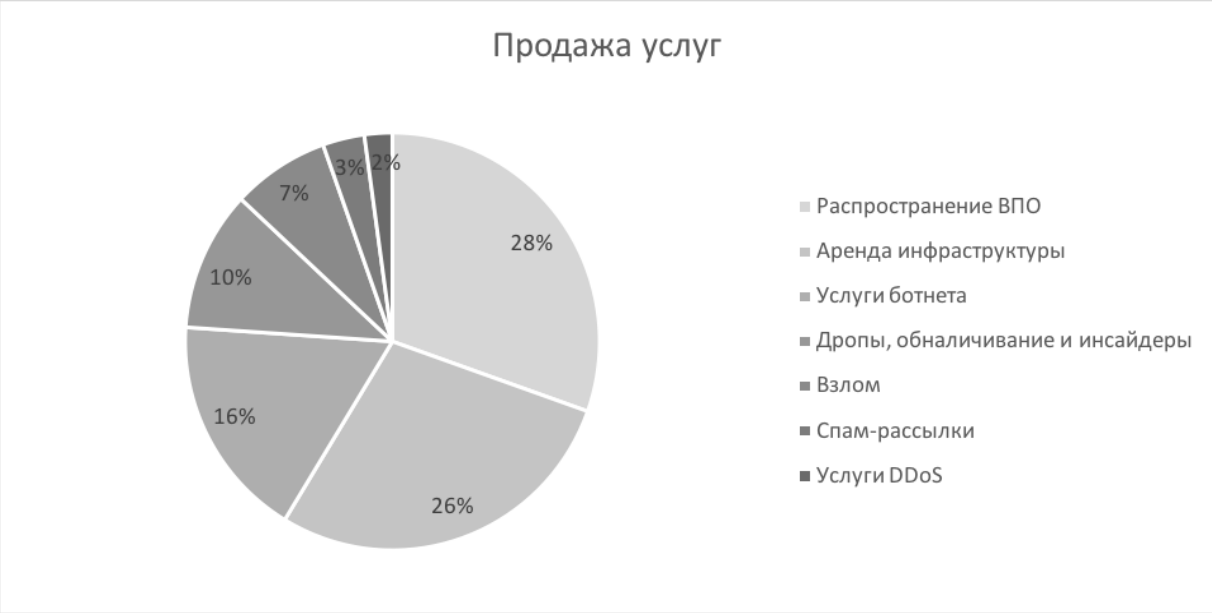

Рис. 3 Процентное соотношение данных о продаже различных услуг для реализации КА в DarkNet
Fig. 3. Percentage of data on the sale of various services for the implementation of CA in DarkNet

2. Этапы компьютерной атаки

В методологиях Cyber Kill Chain [9, 10], NIST 800-115 [12], Certified Ethical Hacker (CEH) [12] под угрозой понимается последовательность этапов действий, начиная с разведки и заканчивая действиями нарушителя по достижению поставленной им цели. Под целью нарушителя подразумевается нарушение конфиденциальности, целостности и/или доступности информации или компонентов информационной системы (ИС) организации. Для каждого этапа нарушитель использует различные методы. Отметим, что методологии NIST 800-115 и Certified Ethical Hacker (CEH) определяют этапы проведения тестирования на проникновение, т.е. эмулирование. Выделенные авторами этапы проведения КА в соответствии методологиями Cyber Kill Chain, NIST 800-115, Certified Ethical Hacker (CEH) приведены в табл. 1.

Из табл. 1 видно, что у обсуждаемых методологий имеется первый общий этап, не связанный с воздействием нарушителя на объект КА – этап теоретической подготовки. В рамках этого этапа нарушителем занимается сбором общедоступной информации, а также изучением инструментов и методов реализации атак. Данная работа схожа с работой исследователя, поэтому, даже, выявив подобную активность, достаточно трудно привлечь нарушителя к ответственности. Второй этап – практическая подготовка, который хоть и связан с активными действиями нарушителя, направленными на объект КА, однако, не приносит «видимого» вреда, а значит, не приводит к обнаружению – обращению в правоохранительные органы [8, 19]. Третий этап, связан с непосредственным нарушением свойств критической (защищаемой) информации. Особенность двух последних этапов заключается в том, что выявленная на первом этапе уязвимость и подготовленный эксплойт по ее эксплуатации на этапе практической реализации КА не гарантирует получение нарушителем запланированного результата. Соответственно, в ходе реализации КА присутствует «петля» или откат к предыдущему этапу для дополнительной подготовки.

Таблица 1. Этапы КА, выделенные в соответствие с методологиями Cyber Kill Chain NIST 800-115, Certified Ethical Hacker (CEH)

Обобщенные этапы КА	Cyber Kill Chain [9, 10]	NIST 800-115 [12]	Certified Ethical Hacker (CEH) [13]
Теоретическая подготовка – объединяет этапы, связанные с изучением объекта КА и подготовкой к КА	Этап «Reconnaissance» – Разведка. Включает исследование, идентификацию и выбор объекта КА. Этап «Weaponization» – Вооружение. Включает выбор и подготовку инструментов и ВПО для совершения КА.	Этап «Planning phase» – Планирования. Определяются правила, а также устанавливаются цели тестирования. Этап «Discovery phase» включает 2 части. Первая часть – это начало реального тестирования и охватывает сбор и сканирование информации. Вторая часть – это анализ уязвимостей, который включает сравнение служб, приложений и операционных систем просканированных узлов с базами данных уязвимостей	Этап «Reconnaissance» – Пассивная и активная разведка. Предполагает сбор информации о потенциальном объекте КА без обнаружения, включая сбор информации с общедоступных источников, отслеживание сетевого трафика и зонирование сети организации. Этап «Scanning» – Сканирование. Подтверждение информации, обнаруженной во время разведки, и ее использование для исследования сети
Практическая подготовка – объединяет этапы, связанные с практической реализации подготовитель-ной части КА	Этап «Delivery» – Доставка. Донесение вредоносного контента до целевой системы. Этап «Exploitation» – Эксплуатация уязвимости системы. Этап «Installation» – Инсталляция. Открытие удаленного доступа и другие действия с зараженной системой Этап «Command and Control (C&C)» – Получение управления. Управление зараженной системой.	Этап « Gaining access » – Получение доступа. Этап «Escalating Privileges» – Повышение полномочий доступа. Этап «System Browsing» – Получение доступа/управление целевой системой. Этап «Install Addition Tools» – Установка/запуск дополнительного ПО. На этих этапах проводится проверка идентифицированных на этапе «Discovery phase» уязвимостей путем их эксплуатации	Этап «Gaining access» – Получение доступа. Уязвимости, обнаруженные на этапе разведки и сканирования, используются для получения доступа к целевой системе
Достижение цели КА – связано с практической реализацией цели КА, в том числе, причинение вреда	Этап «Actions on Objective» – Выполнение действий. Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных.	Этап «Reporting» – Подготовка отчета. Фиксация уязвимостей, эксплуатация которых может привести к успешной реализации реальной КА	Этап «Maintainig access» – реализация цели КА. Получение управления, сохранение доступа для будущих КА и реализация текущих целей КА.

Отметим, что методики КА, связанные с сокрытием следов присутствия нарушителя, мы не выделяем в отдельный этап КА, так как нарушитель стремится их использовать на каждом этапе проведения КА. Кроме того, нарушитель может защищать целевую систему от других нарушителей или специалистов по защите информации,

поддерживая свой эксклюзивный доступ с помощью специального ПО, например, с целью получения выкупа.

В соответствии с технологией Cyber Kill Chain [9, 10] известно, что прервать атаку можно на любом из этапов, тем самым разорвав цепочку действий нарушителя, ведущих его к цели КА. Данные методологии рассматривают КА, в первую очередь, с точки зрения подбора механизмов и средств защиты, но его можно рассмотреть и с точки зрения нарушителя. КА может быть технически прекращена нарушителем:

– если у него будет недостаточно навыков, методов и инструментов для КА, либо они не будут успешно реализовываться на любом из этапов КА.

– если КА будет обнаружена на этапе теоретической или практической подготовки.

3. Обоснование выбора математической модели, описывающей компьютерную атаку

Для моделирования КА обратимся к общей практике выявления и предупреждения правонарушений. В середине 70-х гг. был предложен подход, получивший название «средовое проектирование» [7, 20, 21]. В соответствие с данным подходом полагают, что:

1. Преступления привязаны к местам, наиболее посещаемым преступником – в терминах «средового проектирования» «узлам», к которым традиционно относят места работы, учебы, проживания и т.п. [21].

2. Совокупность мест, находящихся на маршруте передвижения потенциального нарушителя между узлами (например, остановки общественного транспорта, пешеходные дороги и т.п.) называется «тропа». Объекты, находящиеся рядом с тропами также рассматриваются как потенциальные места для совершения преступления (например, парки, магазины по пути следования потенциального нарушителя).

3. Граница минимальной области, охватывающей все «узлы» и «тропы», называется «границей среды» (далее – «граница»).

Принимая во внимание, очевидную аналогию между поведением обычного преступника и преступника, совершающего киберпреступления, можно установить следующее соответствие между ключевыми элементами «средового проектирования» в киберпространстве:

1. «Узлы» – *ip*-адреса нарушителя, прокси-серверы, форумы для получения информации об КА, объекты организации, доступ к которым был получен на успешно реализованных этапах КА, сканируемые или периодически атакуемые для проверки ИС.

2. «Тропы» – маршруты, *TCP* соединения, ИС, к которым есть доступ у нарушителя, наличие выполненных этапов *КА*.

3. «Границы» – объекты, ИС организации, находящиеся в контакте с «узлами» или «тропами». «Граница» определяет область зараженных узлов сети Интернет.

Подтверждением возможности и эффективности применения подхода «средового проектирования» для киберпространства при выявлении вероятных мест КА являются результаты [22, 23], в которых продемонстрировано, что ограничение области анализа уязвимостей ИБ поиском только уязвимых частей программного кода (например, элементов взаимодействия с внешними системами, пользовательских интерфейсов) позволяет улучшить качество прогнозирования новых уязвимостей. Таким образом, рассмотрение точек наиболее вероятного взлома ИС, позволяет улучшить качество прогноза, используемого для выявления новых уязвимостей ПО и оценок векторов КА.

В терминологии выбранного подхода («средового проектирования») правила проведения КА имеют следующие формулировки.

1. Каждый из «узлов» организации, с которым связан нарушитель, становится для него потенциальным началом «тропы» до другого «узла» – объекта КА (т.е. при успешной реализации хотя бы одного из этапов КА нарушитель при достаточности ожидаемой полезности совершит атаку).
2. Ключевым фактором выбора объекта КА является попадание объекта организации в «границы».
3. Успешная реализация КА на внешний «узел» организации предшествует успешной реализации КА на внутренний «узел» организации. Переход нарушителя с одного этапа КА на другой этап КА приводит к расширению «границ».
4. Распространение КА происходит с одного или нескольких «узлов», но не возникает из неоткуда.
5. Правило перехода от «узла» к «узлу» представляет собой или метод реализации КА, или метод получения информации об объекте КА, то есть, де-факто, определяет ключевые факторы КА.
6. Вероятность реализации КА увеличивается при увеличении числа «узлов» и «троп», известных нарушителю.
7. Начальное состояние «узлов» определяет результат реализации метода КА, выбранного нарушителем.

Для обоснования выбора математической модели, описывающей КА, сравним структуры атакуемой ИС, терминологии и правила, используемые в моделировании КА, с соответствующими структурами, терминологией и правилами, используемыми в теории клеточных автоматов [24, 25] (табл. 2).

Из табл. 2 видно, что динамика КА, действительно, подобна динамике клеточного автомата, поэтому изменение состояния отдельного узла ИС в процессе проведения КА можно характеризовать некоторым вероятностным коэффициентом – весовым коэффициентом перехода (ВКП), аналогично тому, как это реализуется в теории клеточных автоматов. Применительно, к КА данный коэффициент, как очевидно, есть ничто иное как показатель вероятности реализации КА.

4. Параметры, влияющие на возможность реализации компьютерной атаки

В [1] обоснована адекватность использования факторов КА для прогнозирования КА. Для построения функциональной зависимости удобнее использовать параметры. Основываясь на логических утверждениях, приведенных в данной статье, представим факторы КА [1] в виде параметров, которые будут определять ВКП.

1. КА может быть начата нарушителем, если:

– нарушителю известен метод КА, в том числе из сети DarkNet (количественно данный фактор можно охарактеризовать коэффициентом a_n известности метода КА, зависящего от активности обсуждений («объяснений») данного метода КА на форумах DarkNet, который есть отношение числа всех обсуждений в указанном сегменте Интернет данного метода КА к общему числу обсуждаемых методов КА);

– на объекте КА отсутствуют или недостаточны меры защиты от данной КА (количественно данный фактор можно охарактеризовать коэффициентом D_a наличия/достаточности средств защиты от данной КА, оценка значения которого может быть получена на основе анализа статистической информации о зафиксированных КА);

– на объекте КА отсутствуют или недостаточны мероприятия по мониторингу КА (количественно данный фактор можно охарактеризовать коэффициентом M_a наличия

решений по мониторингу данной КА, оценка значения которого может быть получена на основе анализа статистической информации о зафиксированных КА).

Таблица 2. Сравнение подходов к описанию динамики атакуемой ИС и клеточного автомата

Структура, термины и правила, используемые в моделировании КА	Структура термины и правила, используемые в теории клеточных автоматов
КА на ИС, состоящую из отдельных (дискретных) узлов, реализуется в соответствие со сценарием КА, предусматривающим некоторую дискретную последовательность действий атакующего (этапов сценария КА). При этом каждый следующий этап КА начинается только после окончания предыдущего этапа КА, а КА распространяется в ИС, через узлы ИС (локальной сети или сети Интернет), связанных друг с другом с помощью троп.	Клеточный автомат – дискретная динамическая систем, представляющая собой совокупность одинаковых клеток, состояние которых зависит от состояния соседних клеток.
Правила проведения КА: – «мгновенное» состояние атакуемой ИС, определяется совокупностью «мгновенных» состояний каждого из узлов ИС; – динамика атакуемой ИС описывается упорядоченной во времени последовательностью «мгновенных» состояний узлов ИС; – изменение/сохранение состояния на данном временном шаге всех узлов атакуемой ИС происходит одновременно; – изменение/сохранение состояний данного узла атакуемой ИС определяется состоянием его соседних узлов ИС (здесь под соседним узлом понимаем не физически, но логически связанные друг с другом узлы атакуемой ИС); – количество состояний каждого из узлов атакуемой ИС конечно.	**Правила изменения состояния клеточного автомата:** – «мгновенное» состояние клеточного автомата определяется совокупностью мгновенных состояний каждой из его клеток; – динамика состояния клеточного автомата описывается упорядоченной во времени последовательностью его «мгновенных состояний»; – изменение/сохранение состояния на данном временном шаге всех клеток происходит одновременно; – изменение/сохранение состояний данной клетки клеточного автомата определяется состоянием ее соседних узлов; – количество состояний каждой клетки клеточного автомата конечно.
Динамика КА полностью определяется: – наличием возможности заражения одного из узлов атакуемой ИС, обусловленной наличием уязвимости, средств защиты и т.п. (начальные условия) – правилами изменения/сохранения свойств узлов атакуемой ИС (при этом число состояний узла атакуемой ИС для разных типов КА количество состояний может быть различным); – числом узлов атакуемой ИС.	Динамика клеточных автоматов полностью определяется: – начальными условиями; – правилами изменения/сохранения свойств клеток; – числом клеток, образующими клеточный автомат.

2. КА может быть прекращена нарушителем, если:

– у нарушителя окажется недостаточно навыков, методов и инструментов для проведения успешной КА, что может быть обнаружено им на любом из этапов КА (количественно данный фактор характеризуется введенными выше коэффициентами a_n и D_a);

– КА будет обнаружена на этапе теоретической или практической подготовки к ее проведению, либо в момент достижения цели КА (количественно данный фактор можно охарактеризовать коэффициентом наличия отсутствия/наличия видимого вреда от КА S_a,

зависящим от использования методов сокрытия при реализации КА нарушителем, который может быть оценен на известности методов сокрытия в сети DarkNet S_a, а также ранее введенным коэффициентом M_a);

3. КА может быть прекращена специалистом по защите информации, если:

– КА будет обнаружена на этапе ее теоретической или практической подготовки, либо в момент достижения цели КА (количественно данный фактор можно охарактеризовать коэффициентом T – длительностью временного интервала, необходимого для обнаружения КА и разработки рекомендаций по блокировке КА и соответствующих средств защиты от КА, в частности, новых вирусных сигнатур);

– существует (либо находится в финальной стадии разработки) решение по защите от данной КА (количественно данный фактор можно охарактеризовать ранее введенным параметром D_a, а также числом узлов атакуемой ИС $У_a$, потенциально подверженных данной КА, и общим числом узлов атакуемой ИС $У$ в сети Интернет).

Таким образом, ВКП, определяющий динамику КА на ИС, является функцией, зависящей от переменных $У_a, У, T, D_a, M_a, S_a, a_a$:

$$ВКП = F\left(У_a, У, T, D_a, M_a, S_a, a_a\right). \quad (2)$$

Для подтверждения адекватности предложенных авторами подходов далее был проведен анализ КА, реализованной ВПО Petya на ИС, расположенные на территории Украины, результаты которого обсуждаются далее. Обоснование выбора конкретного типа функции $F\left(У_a, У, T, D_a, M_a, S_a, a_a\right)$ является предметом дальнейших исследований.

5. Анализ сценария компьютерной атаки, реализованной с помощью вредоносного программного обеспечения Petya

Напомним, что распространение ВПО Petya началось в апреле 2017 г. [20]. Данное ПО использовало известную на тот момент уязвимость EternalBlue, которая ранее уже эксплуатировалась для проведения КА шифровальщиком WannaCry. Это, с нашей точки зрения, является подтверждением наличия этапа «Практическая подготовка к проведению КА». Данный вывод также подтверждается результатами анализа форумов и чатов DarkNet в соответствующий период времени [18], результаты которого свидетельствуют о том, что:

– осуществлялась продажа услуг, связанных, с подготовкой поддельных файлов якобы с обновлениями или утилитами, которые размещают на взломанных или подконтрольных нарушителю организациях в 51% случаев (из всех услуг продаваемых в DarkNet);

– происходило обсуждение ВПО, связанного с Троянами-вымогатели (ransomware), к которым относится Petya (процент сообщений, связанных с этим типов ВПО составлял 12%).

В доступном описании сценария КА ВПО Petya на ИС, расположенные на территории Украины [19], в том числе сообщается.

«Заражение вирусом началось через распространение обновления для ПО M.E.Doc 27 июня 2017 г. ПО M.E.Doc широко используется для подачи бухгалтерской отчетности на Украине, по данным специалистов информационной безопасности, у фирмы на момент заражения было около 400 тысяч клиентов, что составляет порядка 90 % всех организаций страны.» [19, 20] Таким образом, об КА стало известно только 27.06.2017, а именно от организаций Украины с 27.06.2017 по 28.06.2017: «в Департамент киберполиции Украины

поступило более 1000 сообщений о вмешательстве в работу компьютерных сетей, что привело к сбоям в их работе. Из них официально с заявлениями в полицию обратились 43 компании» [7].

Полный перечень мероприятий по защите от этой КА был разработан в течение суток после обнаружения КА [25]. «28 июня 2017 г. Кабинет Министров Украины сообщил, что масштабная КА на корпоративные сети и сети органов власти была остановлена. 4 июля 2017 г. с целью немедленного прекращения распространения червя Petya принято решение о проведении обысков и изъятии программного и аппаратного обеспечения компании, с помощью которого распространялось ВПО. Обыски проведены представителями Департамента киберполиции, следователями и при участии Службы безопасности Украины. Изъяты рабочие компьютеры персонала и серверное оборудование, через которое распространялось ПО» [7].

Таким образом, КА ВПО Petya было реализовано в 3 этапа.

1. Теоретическая подготовка, состоящая в анализе сетей DarkNet и планировании данной КА.

2. Практическая подготовка, состоящая в доставке ВПО до целевой системы в период с апреля по июнь 2017 г., которая охватило порядка 90% всех узлов украинских ИС.

3. Достижение цели КА (напомним, что видимый ущерб был обнаружен 27.06.17, еще сутки потребовались для формирования перечня мероприятий по защите и еще 8 дней для окончательного блокирования КА).

Таким образом, обсуждаемая КА характеризуется:

– количеством атакованных узлов украинских ИС (90% от их общего числа) (в (2) – переменная $У_a$).

– общим количеством узлов украинских ИС в сети Интернет (в (2) – переменная У);

– временем, потребовавшимся для обнаружения КА (3 месяца) и разработки рекомендаций по его блокировке (1 день) (в (2) – переменная T);

– отсутствие/недостаточность соответствующих средств защиты на момент начала КА (в (2) – переменная D_a);

– отсутствие/недостаточность средств мониторинга данной КА (в (2) – переменная M_a);

– использование методов сокрытия КА на начальном этапе проведения (в (2) – переменная S_a);

– использованием известной уязвимости украинских систем ИБ ИС (коэффициент известности метода КА (в (2) – a_n, оказавшийся равным составил 31,5%).

Заключение

В статье на основе анализа существующих методологий Cyber Kill Chain, Mitre Att&ck, NIST 800-115, Certified Ethical Hacker (CEH), ФСТЭК России и ISO 27001, регламентирующих этапы и методы реализации КА, выявлены с точки зрения нарушителя следующие этапы КА:

1. Теоретическая подготовка.
2. Практическая подготовка.
3. Достижение цели КА.

Проведен сравнительный анализ математических подходов, используемых для описания динамики атакуемой ИС и клеточного автомата, результаты которого позволил

сделать обоснованный вывод о том, что динамика КА подобна динамике клеточного автомата.

Предложено использовать, аналогично тому, как это реализуется в теории клеточных автоматов, для изменения состояния отдельного узла ИС в процессе проведения КА, вероятностного коэффициента, названного весовым коэффициентом перехода, который является функцией, зависящей от обоснованно выбранных количественных показателей КА.

Достаточность перечня выбранных количественных показателей подтверждена результатами анализа сценария КА ВПО Petya на ИС, расположенные на территории Украины.

СПИСОК ЛИТЕРАТУРЫ:

1. Макарова, Ольга С., Поршнев, Сергей В. Оценивание вероятностей компьютерных атак на основе метода анализа иерархий с динамическими приоритетами и предпочтениями. Безопасность информационных технологий, [S.l.]. Т. 27, № 1. С. 6–18, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1248 (дата обращения: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.01.
2. O. Makarova and S. Porshnev. Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information, 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2020. P. 593–596. DOI: http://dx.doi.org/10.1109/USBEREIT48449.2020.9117676.
3. Макарова, Ольга С., Поршнев, Сергей В. Оценивание вероятностей компьютерных атак на основе функций Безопасность информационных технологий, [S.l.], Т. 27, № 2. С. 86–96. SSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1273 (дата обращения: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.07.
4. Hausken K., Moxnes J.F The dynamics of crime and punishment // International Journal of Modern Physics C. 2005. Vol. 16, no. 11. P. 1701–1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
5. Becker G.S. The economics of crime // Cross Sections, Federal Reserve Bank of Richmond. 1995. Vol. 12. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (дата обращения: 27.04.2020).
6. Бернулли Д. Опыт новой теории измерения жребия. Вехи экономической мысли. Теория потребительского поведения и спроса. Под ред. В.М. Гальперина. СПб.: Экономическая школа, 1999. Т. 1. С. 11–27.
7. Vagi KJ, Stevens MR, Simon TR, Basile KC, Carter SP, Carter SL. Crime Prevention Through Environmental Design(CPTED) characteristics associated with violence and safety in middle schools. J Sch Health. 2018. Vol. 88. P. 296–305. DOI: https://doi.org/10.1111/josh.12609.
8. Хакерские атаки на Украину (2017). URL: https://www.protectimus.com/blog/ru-conclusions-hacking-attacks-ukraine/ (дата обращения: 29.12.2020).
9. Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hack Tech 15, 277–305 (2019). DOI: https://doi.org/10.1007/s11416-019-00338-7.
10. The Cyber Kill Chain, lockheedmartin.com. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 29.12.2020).
11. Enterprise Matrix, attack.mitre.org. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 29.12.2020).
12. Scarfone, Karen & Souppaya, Murugiah & Cody, Amanda & Orebaugh, Angela. (2008). NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. URL: https://www.researchgate.net/publication/329973439_NIST_Special_Publication_800-115_Technical_Guide_to_Information_Security_Testing_and_Assessment (дата обращения: 29.12.2020).
13. Certified Ethical Hacker, eccouncil.org. URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (дата обращения: 29.12.2020).
14. Методика определения актуальных угроз безопасности персональных данных при их обработке в ИС персональных данных. М.: ФСТЭК России, 2008. – 10 с.
15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). М.: ФСТЭК России, 2008. – 69 с.

16. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p.
17. Банк данных угроз БИ ФСТЭК России // FSTEC.RU/ URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2019).
18. Positive Technologies. Рынок преступных киберуслуг 2018. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf (дата обращения 11.11.2020).
19. Спецслужбы ФРГ: вирус Petya позволяет красть данные Вредоносное ПО в Германии распространялось через уязвимость в программе украинского разработчика. URL: https://tass.ru/mezhdunarodnaya-panorama/4396011 (дата обращения: 29.12.2020).
20. Разогреева А.М. Предупреждение преступлений при помощи средового проектирования: защищающее пространство и защищенное пространство / А.М. Разогреева // Всероссийский криминологический журнал. 2017. Т. 11, № 4. С. 706–716. DOI: https://doi.org/10.17150/2500-4255.2017.11(4).706-716.
21. Бауман З. Текучая современность/Пер. с англ. под ред. Ю.В. Асочакова. СПб.: Питер, 2008. – 240 с.
22. J. Stuckman, J. Walden and R. Scandariato. The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models, in IEEE Transactions on Reliability. 2017. Vol. 66, no. 1. P. 17–37. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
23. Нейман Дж. Теория самовоспроизводящихся автоматов / Дж. фон Нейман; закончено и отредактировано А. Бёрксом; пер. с англ. В. Л. Стефанюка; под ред. и с предисл. В. И. Варшавского. - Изд. 2-е. М.: URSS: Либроком, 2009. – 382 с.
24. Макарова, О. С. Моделирование непреднамеренного распространения информации пользователем / О.С. Макарова. Текст: непосредственный // Технические науки: проблемы и перспективы: материалы I Междунар. науч. конф. (г. Санкт-Петербург, март 2011 г.). СПб.: Реноме, 2011. С. 99–103. URL: https://moluch.ru/conf/tech/archive/2/136/ (дата обращения: 29.12.2020).
25. Новая эпидемия шифровальщика Petya / NotPetya / ExPetr. URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/ (дата обращения: 29.12.2020).

REFERENCES:

[1] Makarova, Olga S., Porshnev, Sergey V. Assessment of probabilities of computer attacks based on the method of analysis of hierarchies with dynamic priorities and preferences. IT Security (Russia), [S.l.]. Vol. 27, no. 1. P. 6–18, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1248 (accessed: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.1.01 (in Russian).
[2] O. Makarova, S. Porshnev, Assessment of Probabilities of Computer Attacks Based on Analytic Hierarchy Process: Method for Calculating the Pairwise Comparison Matrixs Based on Statistical Information, Conference paper, 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Institute of Electrical and Electronics Engineers Inc., 2020. P. 593–596. DOI: http://dx.doi.org/10.1109/USBEREIT48449.2020.9117676.
[3] Makarova, Olga S., Porshnev, Sergey V. Assessment of probabilities of computer attacks based on function. IT Security (Russia), [S.l.]. Vol. 27, no. 2. P. 86-96, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1273 (accessed: 29.12.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.07 (in Russian).
[4] Hausken K., Moxnes J.F The dynamics of crime and punishment. International Journal of Modern Physics C. 2005. Vol. 16, no. 11. P. 1701–1732. DOI: http://dx.doi.org/10.1142/S0129183105008229.
[5] G. Becker. The economics of crime, Cross Sections, Federal Reserve Bank of Richmond. Vol. 12, 1995. P. 8–15. URL: https://ideas.repec.org/a/fip/fedrcs/y1995ifallp8-15nv.12no.3.html (accessed: 27.04.2020).
[6] D. Bernoulli. Experience of a new theory of measurement of lots. Theory of consumer behavior and demand. Milestones of economic thought. Edited by V.M. Galperin. SPb.: Ekonomicheskaya shkola, 1999. P. 11–27 (in Russian).
[7] Vagi KJ, Stevens MR, Simon TR, Basile KC, Carter SP, Carter SL. Crime Prevention Through Environmental Design(CPTED) characteristics associated with violence and safety in middle schools. J Sch Health. 2018. Vol. 88. P. 296–305. DOI: https://doi.org/10.1111/josh.12609.
[8] Hacker attacks on Ukraine (2017). URL: https://www.protectimus.com/blog/ru-conclusions-hacking-attacks-ukraine/ (accessed: 29.12.2020) (in Russian).
[9] Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hack Tech 15, 277–305 (2019). DOI: https://doi.org/10.1007/s11416-019-00338-7.

[10] The Cyber Kill Chain, lockheedmartin.com. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed: 29.12.2020).
[11] Enterprise Matrix, attack.mitre.org. URL: https://attack.mitre.org/matrices/enterprise/ (accessed: 29.12.2020).
[12] Scarfone, Karen & Souppaya, Murugiah & Cody, Amanda & Orebaugh, Angela. (2008). NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. URL: https://www.researchgate.net/publication/329973439_NIST_Special_Publication_800-115_Technical_Guide_to_Information_Security_Testing_and_Assessment (accessed: 29.12.2020).
[13] Certified Ethical Hacker, eccouncil.org. URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (accessed: 29.12.2020).
[14] Actual threats definitions method to personal data security during their processing in the information systems of personal data. M.: FSTEC Russia, 2008. – 10 p. (in Russian).
[15] The threats basic model to personal data security during their processing in personal data information systems (extract), M.: FSTEC Russia, 2008. – 69 p. (in Russian).
[16] ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. M.: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2013. – 23 p.
[17] Information security threats databank of FSTEC Russia, FSTEC.RU URL: https://bdu.fstec.ru/ (accessed: 29.12.2020) (in Russian).
[18] Positive Technologies. Criminal cyber services market, ptsecurity.com. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Darkweb-2018-rus.pdf (accessed: 29.12.2020) (in Russian).
[19] German intelligence services: Petya virus allows data to be stolen, tass.ru. URL: https://tass.ru/mezhdunarodnaya-panorama/4396011 (accessed: 29.12.2020) (in Russian).
[20] Razogreeva A.M. Crime prevention through environmental design: defensible space and protected space. Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology. 2017. Vol. 11, no. 4. P. 706–716. DOI: https://doi.org/10.17150/2500-4255.2017.11(4).706-716 (in Russian).
[21] Z. Bauman, Liquid modernity. Polity Press, 2000. – 225 p.
[22] J. Stuckman, J. Walden, R. Scandariato. The Effect of Dimensionality Reduction on Software Vulnerability Prediction Models, in IEEE Transactions on Reliability. 2017. Vol. 66, no. 1. P 17–37. DOI: http://dx.doi.org/10.1109/TR.2016.2630503.
[23] John Von Neumann and Arthur W. Burks. Theory of Self-Reproducing Automata. University of Illinois Press, USA. 1966. – 408 p.
[24] Makarova, O.S. Modeling of unintentional dissemination of information by the user. O.S. Makarova. Text: direct. Technical sciences: problems and prospects: materials of the I International Scientific Conference (SPb., March 2011). StPb.: Renome, 2011. P. 99–103. URL: https://moluch.ru/conf/tech/archive/2/136 (accessed: 29.12.2020) (in Russian).
[25] New Petya. NotPetya. ExPetr ransomware epidemic, kaspersky.ru. URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/ (accessed: 29.12.2020) (in Russian).

Поступила в редакцию – 14 января 2021 г. Окончательный вариант – 22 марта 2021 г.
Received – January 14, 2021. The final version – March 22, 2021.