УДК 004.056.53

ОЦЕНКА ПОТЕНЦИАЛЬНЫХ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ ОРГАНИЗАЦИЙ ЭЛЕКТРОСВЯЗИ

В.А. БОЙПРАВ, Л.Л. УТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 18 марта 2019

Аннотация. Проанализированы потенциальные уязвимости информационных систем и сетей, используемых организациями электросвязи. В соответствии со стандартом CVSS v3 выполнена оценка этих уязвимостей. Представлен анализ этой оценки.

Ключевые слова: организации электросвязи, угроза, уязвимость.

Введение

Одним из наиболее важных критериев, используемых для оценки защищенности информационных систем и сетей, является качество системы ее мониторинга, которая представляет собой совокупность мероприятий, направленных на выявление потенциальных угроз информационной безопасности. Важность указанного критерия обусловлена тем, что на нем базируется процесс построения эффективной системы защиты информации, который включает в себя определение комплекса организационных и технических мер, направленных на обеспечение конфиденциальности, доступности, целостности, подлинности и сохранности данных, циркулирующих в информационной системе или сети, а также принципы и порядок (очередность) внедрения этих мер.

Очередность внедрения каждой из мер как элемента системы защиты информации определяется критичностью реализации потенциальной угрозы информационной безопасности, на устранение которой направлена эта мера. Для определения указанной очередности необходимо в процессе мониторинга информационных систем и сетей выполнять построение моделей потенциальных угроз безопасности циркулирующих в них данных. Оно заключается в описании следующих свойств каждой из таких угроз [1]: уязвимость информационной системы и сети, на которую воздействует угроза; источник угрозы; способ реализации угрозы (принцип воздействия угрозы на уязвимость); последствия от реализации угрозы.

Первое из указанных свойств является базовым для определения критичности реализации потенциальной угрозы информационной безопасности.

В рамках представляемой работы выполнена оценка уязвимостей информационных систем и сетей организаций электросвязи, для чего были решены следующие задачи:

1. определение перечня потенциальных уязвимостей информационных систем и сетей организаций электросвязи;
2. выбор и обоснование методики оценки потенциальных уязвимостей;
3. анализ полученных результатов оценки.

Актуальность представляемой работы обусловлена тем, что информационные системы и сети организаций электросвязи являются критически важными объектами информатизации (КВОИ) либо элементами инфраструктуры таких объектов, в связи с чем от степени защищенности этих систем и сетей зависит состояние национальной безопасности.

Анализ потенциальных уязвимостей информационных систем и сетей организаций электросвязи

В работе [2] выделены следующие группы активов информационных систем и сетей организаций электросвязи: аппаратные, программные, аппаратно-программные, обрабатываемая

информация, информационные процессы. В табл. 1 представлен перечень основных активов информационных систем и сетей организаций электросвязи различных сфер деятельности.

Таблица 1. **Активы информационных систем и сетей организаций электросвязи различных сфер деятельности**

Сфера деятельности организации электросвязи	Наименование группы активов информационных систем и сетей	Основные активы информационных систем и сетей
Проектирование сетей и сооружений электросвязи	Программные	Программное обеспечение, используемое для проектирования сетей и сооружений электросвязи
	Аппаратно-программные	Средства вычислительной техники
	Обрабатываемая информация	Схемы разработанных или разрабатываемых проектов
	Информационные процессы	Создание, хранение, передача
Строительство сетей и сооружений электросвязи	Аппаратные	Линии и средства электросвязи
Предоставление услуг электросвязи	Аппаратные	Средства электросвязи
	Программные	Программное обеспечение для работы с базами данных и для защиты информации
	Аппаратно-программные	Средства вычислительной техники
	Обрабатываемая информация	Данные об абонентах
	Информационные процессы	Создание, хранение
Государственное регулирование и управление в области электросвязи	Программные	Программное обеспечение для организации электронного документооборота и защиты информации
	Аппаратно-программные	Средства вычислительной техники
	Обрабатываемая информация	Документы, регулирующие деятельность в области электросвязи
	Информационные процессы	Создание, хранение, передача

Потенциальные уязвимости информационных систем и сетей обусловлены уязвимостями их активов, а также несоблюдением пользователями этих систем и сетей организаций требований о неразглашении сведений, связанных с особенностями их функционирования и эксплуатации, а также с содержанием обрабатываемой информации.

Потенциальные уязвимости аппаратных и аппаратно-программных активов могут быть связаны со следующими особенностями их реализации и эксплуатации:

– выход из строя ввиду производственных дефектов;

– некорректное подключение;

– несвоевременность устранения повреждений;

– незащищенность от побочного электромагнитного излучения.

Причинами потенциальных уязвимостей программных активов могут быть следующие:

– ошибки в программных кодах, позволяющие злоумышленнику реализовать несанкционированный доступ в информационную систему или сеть либо внедрить вредоносное программное обеспечение;

– ошибки в программных кодах, приводящие к сбою процессов функционирования программных активов;

– некорректность настроек;

– несовместимость программных активов друг с другом (в том числе с используемыми для управления информационными системами и сетями операционными системами).

Потенциальные уязвимости информационных процессов связаны как с представленными выше уязвимостями, так и с несовершенством используемых алгоритмов шифрования, ошибками проектирования информационной системы или сети.

Методика выполнения оценки потенциальных уязвимостей

Для выполнения оценки потенциальных уязвимостей информационных систем и сетей организаций электросвязи использован стандарт CVSS v3 (от англ. Common Vulnerability Scoring

System version 3). Выбор указанного стандарта обусловлен большим количеством предусмотренных в рамках него метрик уязвимости и соответствующих им характеристик, что позволяет обеспечить высокую точность ее оценки.

Метрики, предусмотренные в стандартах CVSS, делятся на следующие виды:

– базовые (совокупность характеристик уязвимости, не меняющихся со временем);

– временные (совокупность характеристик уязвимости, используемых для описания полноты имеющейся о ней информации, степени зрелости эксплуатирующего ее программного кода);

– контекстные (совокупность характеристик информационной системы или сети, в которой обнаружена уязвимость).

В табл. 2 представлены характеристики, соответствующие метрикам указанных видов, а также описание этих характеристик.

Таблица 2. **Характеристики метрик, предусмотренных стандартом CVSS v3**

Наименование метрик в зависимости от их вида	Наименование характеристики	Обозначение характеристики	Параметры характеристики
Базовые	Attack vector (вектор атаки)	AV	Network (N) Adjacent Network (A) Local (L) Physical (P)
	Attack complexity (сложность атаки)	AC	Low (L) High (H)
	Privileges required (требуемый уровень привилегий)	PR	High (H) Low (L) None (N)
	User interaction (необходимость взаимодействия с пользователем)	UI	None (N) Required (R)
	Scope (границы эксплуатации)	S	Unchanged (U) Changed (C)
	Confidentiality impact, integrity impact, availability impact (метрики воздействия)	C I A	None (N) Medium (M) High (H)
Временные	Exploit code maturity (степень зрелости доступных средств эксплуатации уязвимости)	E	Not Defined (ND/X) High (H) Functional (F)[1] Proof-of-Concept (POC/P)[2] Unproven (U)[3]
	Remediation level (доступные средства устранения уязвимости)	RL	Not Defined (ND/X) Unavailable (U) Workaround (W)[4] Temporary Fix (TF/T)[5] Official Fix (OF/O)[6]
	Report confidence (степень доверия к информации об уязвимости)	RC	Not Defined (X) Unknown (U)[7] Reasonable (R)[8] Confirmed (C)[9]
Контекстные	Confidentiality requirement, integrity requirement, availability requirement (требования к безопасности)	CR IR AR	Not Defined (ND/X) High (H) Medium (M) Low (L)

[1] Имеется программный код для эксплуатации уязвимости
[2] Имеется сценарий реализации атаки
[3] Наличие программного кода для эксплуатации уязвимости не подтверждено
[4] Средства устранения уязвимости разработаны самой организацией (являются неофициальными)
[5] Средства устранения уязвимости являются временно официальными
[6] Средства устранения уязвимости являются официальными
[7] Описание причины уязвимости отсутствует
[8] Существуют отчеты об уязвимости, с помощью которых можно установить причины ее возникновения, а также выполнить ее оценку
[9] Наличие уязвимости подтверждено производителем продукта

Результаты и их обсуждение. Выводы

В табл. 3 представлены вектора наиболее критичных потенциальных уязвимостей информационных систем и сетей организаций электросвязи различных сфер деятельности.

Таблица 3. **Вектора потенциальных уязвимостей информационных систем и сетей организаций электросвязи различных сфер деятельности**

Сфера деятельности организации электросвязи	Вектора основных потенциальных уязвимостей информационных систем и сетей		
	Базовые метрики	Временные метрики	Контекстные метрики
Проектирование сетей и сооружений электросвязи, предоставление услуг электросвязи, государственное регулирование и управление в области электросвязи	AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/	E:F/RL:O/RC:R	CR:H/IR:H/AR:H
Строительство сетей и сооружений электросвязи	AV:P/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H	E:F/RL:W/RC:X	CR:H/IR:M/AR:M

Информационные системы и сети организаций электросвязи, сфера деятельности которых сопряжена с проектированием, предоставлением услуг и государственным регулированием, характеризуются одинаковыми векторами наиболее критичных потенциальных уязвимостей, которые обусловлены уязвимостями программных активов.

На основании анализа полученных векторов потенциальных уязвимостей информационных систем и сетей организаций электросвязи бала выполнена их оценка [3]. В табл. 4 представлены результаты этой оценки.

Таблица 4. **Оценки потенциальных уязвимостей информационных систем и сетей организаций электросвязи различных сфер деятельности**

Сфера деятельности организации электросвязи	Оценки основных потенциальных уязвимостей информационных систем и сетей		
	Базовые метрики	Временные метрики	Контекстные метрики
Проектирование сетей и сооружений электросвязи, предоставление услуг электросвязи, государственное регулирование и управление в области электросвязи	8,0	7,1	7,6
Строительство сетей и сооружений электросвязи	7,1	6,7	6,7

Из табл. 4 следует, что в соответствии со стандартом CVSS v 3, потенциальные уязвимости информационных систем и сетей организаций электросвязи, сфера деятельности которых сопряжена с проектированием, предоставлением услуг и государственным регулированием являются более критичными, чем потенциальные уязвимости систем и сетей, эксплуатируемых организациями, задействованными в строительстве сетей и сооружений электросвязи. Однако класс вторых из упомянутых информационных систем и сетей, как КВОИ, выше, чем класс первых. В связи с этим, по мнению авторов, для того, чтобы использовать стандарт CVSS v 3 для оценки потенциальных уязвимостей информационных систем и сетей организаций электросвязи необходимо использовать поправочные коэффициенты, зависящие от класса этих систем и сетей как КВОИ. Дальнейшие исследования будут направлены на определение и обоснование этих коэффициентов.

ASSESSMENT OF POTENTIAL VULNERABILITIES OF TELECOMMUNICATION ORGANIZATIONS' INFORMATION SYSTEMS AND NETWORKS

V.A. BOIPRAV, L.L. UTIN

Abstract. The potential vulnerabilities of information systems and networks used by telecommunication organizations is analyzed. These vulnerabilities were assessed in accordance with the CVSS v3 standard. An analysis of this assessment is presented.

Keywords: telecommunication organizations, threat, vulnerability.

Список литературы

1. ТКП 483-2013 (01019). Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования. Минск: ОАЦ, 2013. 6 с.
2. Бойправ В.А., Утин Л.Л. Особенности подготовительного этапа аудита системы менеджмента защиты информации в организациях электросвязи // Докл. БГУИР. 2018. № 1 (111). С. 43–50.
3. NVD – CVSS v3 Calculator [Electronic resource]. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (date of access:15.03.2019).