СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ
SYSTEM ANALYSIS AND PROCESSING OF KNOWLEDGE

УДК 004.056 **DOI: 10.18413/2518-1092-2019-4-4-0-3**

Оладько В.С.

ИНЦИДЕНТЫ СЕТЕВОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ЦИФРОВОЙ ЭКОНОМИКИ

Финансовый университет при Правительстве Российской Федерации,
Ленинградский просп., д. 49, г. Москва, 125993 (ГСП-3), Россия

e-mail: vsoladco@fa.ru

Аннотация
Современный период развития тесно связан с цифровой трансформацией различных отраслей деятельности и внедрением в Российской Федерации программы Цифровой экономики. Одним из факторов успешного внедрения и эффективного развития подобной социотехнической системы является обеспечение кибербезопасности объектов и субъектов в процессах обработки и передачи информации, получения цифровых услуг. Поскольку основой информационной инфраструктуры системы цифровой экономки является сетевая подсистема, то исследование проблем обеспечения ее безопасности является важной научно-практической задачей. Целью работы является разработка описательной модели инцидентов сетевой безопасности. Для достижения цели решаются частные задачи: определение требований к безопасности и доверию в системе цифровой экономики; анализ типовой модели сетевого взаимодействия в системе цифровой экономике; описание жизненного цикла инцидентов безопасности и анализ связи инцидента с рисками. Результатом исследования является создание карточки типовых инцидентов сетевой безопасности, которая может быть использована в процессе управления инцидентами безопасности, на этапе их идентификации и профилактики.
Ключевые слова: социотехническая система; угроза; киберезопасность; инциденты безопасности; сетевая атака.

UDC 004.056

Oladko V.S.

NETWORK SECURITY INCIDENTS IN THE DIGITAL ECONOMY SYSTEM

Financial University under the Government of the Russian Federation,
49 Leningradsky prosp., Moscow, 125993 (GSP-3), Russia

e-mail: vsoladco@fa.ru

Abstract
The modern period of development is closely related to the digital transformation of various industries and the implementation of the Digital Economy program in the Russian Federation. One of the factors for the successful implementation and effective development of such a sociotechnical system is ensuring the cybersecurity of objects and entities in the processes of processing and transmitting information, and obtaining digital services. The study of the problems of ensuring its security is an important scientific and practical task, because the basis of the digital economy system is the network subsystem. The aim is to develop a descriptive model of network security incidents. To achieve the goal, the author solves particular problems: determining security requirements and trust in the digital economy system; analysis of a typical model of network interaction in the digital economy system; description of the life cycle of security incidents and an analysis of the association of the incident with the risks. The result of the study is

the creation of a card of typical network security incidents, which the author suggests using in the process of managing security incidents, at the stage of their identification and prevention.
Keywords: sociotechnical system; threat; cybersecurity; security incidents; network attack.

ВВЕДЕНИЕ

Современное общество и государственная политика в различных отраслях деятельности характеризуется процессами активного развития социотехнических систем и трансформации цифровой экономики, целью является стимулирование цифрового производства, создание универсальных порталов и маркетплейсов для эффективного предоставления данных, продуктов и услуг, повышение их качества и совершенствование цифровых технологий и инфраструктуры. Согласно источникам [6, 9, 10] систему цифровой экономики можно разделить на хабы:

1. Государство и общество, включающее цифровое правительство, здравоохранение, образование, культуру и граждан – потребителей услуг.
2. Маркетинг и реклама, включая контент-маркетинг, контекстную, медийную, мобильную и видеорекламу.
3. Финансы и торговля, включая рынок электронной коммерции и онлайн-платежей, онлайн-тревел, онлайн-ретейл.
4. Инфраструктура и связь, включая рынки доменов, хостингов, SAAS, облачных технологий и хранилищ данных.
5. Медиа и развлечения, включая ИКТ-сектор и сектор контента и средств массовой информации.
6. Кибербезопасность.
7. Образование и кадры.

Каждый из представленных хабов представляет собой множество социотехнических систем и вносит вклад в трансформацию экономической системы Российской Федерации. Для выполнения целевых бизнес-процессов используется информационная инфраструктура, которая строится на базе веб-приложений, проводных и беспроводных сетей передачи данных, электронных платежных систем, современных информационно-коммуникационных технологий, включая большие данные, машинное обучение, системы распределённого реестра и блокчейн, квантовые технологии, промышленный интернет и интернет-вещей, виртуальную и дополненную реальности. От надежности и безопасности информационной инфраструктуры будет зависеть качество производимых цифровых товаров и услуг, а также степень доверия участников социотехнической системы цифровой экономики.

Актуальность проблем обеспечения безопасности цифровой экономике нашла свое отражение в работах таких российских ученых как Ершова Т.В., Горулев Д.А., Асаул В.В., Михайлова А.О., Минзов А.С., Невский А.Ю., Баронов О.Ю. Авторами исследуются вопросы, связанные с выявлением сущности цифровой экономики, ее отраслевых элементов, их содержания в рамках современного цифрового общества; проблемами экономической безопасности, доверием и кибербезопасностью. В этом контексте недостаточно проанализированными остаются аспекты, связанные с анализом инцидентов информационной безопасности при сетевом взаимодействии субъектов и объектов цифровой экономики.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

В работе автором в качестве объекта исследования была выбрана сетевая подсистема информационной инфраструктуры цифровой экономики. Предметом исследования – вопросы, связанные с обеспечением безопасности сетевого взаимодействия участников системы цифровой экономики.

Цель работы – разработать модель инцидентов сетевой безопасности. Поставленная цель работы обуславливает необходимость решения основных задач:

- определение требований к безопасности и доверию в системе цифровой экономики;
- анализ типовой модели сетевого взаимодействия в системе цифровой экономике;

- разработка модели инцидентов сетевой безопасности.

МАТЕРИАЛЫ И МЕТОДЫ ИССЛЕДОВАНИЯ

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, элементы теории множества.

Требования к безопасности и доверию в системе цифровой экономики

Согласно Плану мероприятий по направлению «Информационная безопасность»[1] программы «Цифровая экономика Российской Федерации», утвержденному Правительственной комиссией, протокол от 18 декабря 2017 г. №2 взаимодействие и доверие субъектов в цифровой экономики невозможно без реализации мер и технологий обеспечения информационной безопасности на всех уровнях информационного пространства. Меры должны способствовать достижению целевых показателей и индикаторов безопасности и охватывать вопросы, связанные с безопасностью информационной инфраструктуры и повышением доверия граждан и бизнеса к цифровым технологиям и сервисам (рис. 1).

Рис. 1. Направления деятельности по обеспечению безопасности и доверия в цифровой экономике
Fig. 1. Security and trust areas in the Digital Economy

Направление обеспечения сетевой безопасности, охватывает вопросы контроля внутреннего и внешнего трафика субъектов и объектов, обеспечения безопасности функционирования российского сегмента сети Интернет, обнаружения и противодействия сетевым кибератакам, в том числе через IIoT-устройства [18], предотвращения утечек информации ограниченного доступа [6], сегментации сети [8] и построения доверенных сред [6].

[1] План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации», утвержден Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18 декабря 2017 г. №2). [Электронный ресурс]. URL: http://www.tadviser.ru/images/5/53/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf

Типовая модель сетевого взаимодействия объектов системы цифровой экономики

Сетевая подсистема информационной инфраструктуры имеет распределённую клиент-серверную с выходом в сеть общего пользования, удаленными веб-серверами, хранилищами данных и пользователями (см. рисунок 2), которая окружена существенной средой [11], порождающей угрозы безопасности случайного или умышленного характера.

Сетевое взаимодействие субъектов основывается на процессах передачи данных в виде множества пакетов, образующих сетевой трафик. Правила фрагментации и передачи описывает эталонная модель взаимосвязи открытых систем (модель OSI), которая представляет базис и содержит два [12-14] основных принципа (см. рис. 2):

- все открытые системы имеют многоуровневую архитектуру, включающую в себя семь уровней;
- для всех передаваемых данных проводится инкапсуляция/декапсуляция.

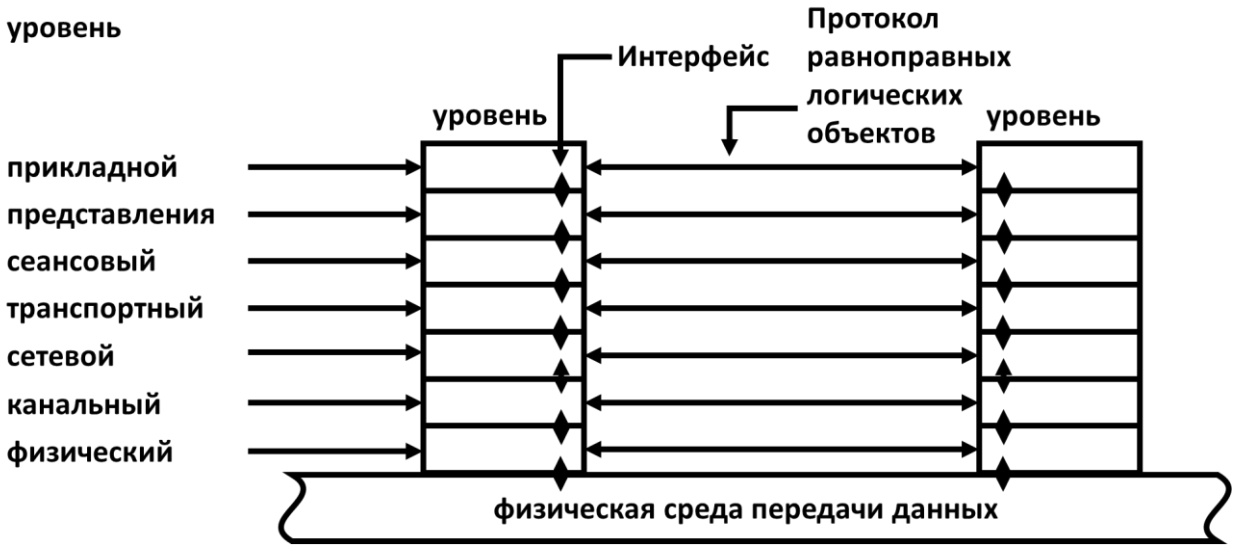

Рис. 2. Уровни модели OSI
Fig. 2. OSI model levels

Самым верхним является прикладной уровень, или уровень приложений. Самым нижним – физический, подразумевающий под собой физическую среду передачи данных. Все объекты сетевой подсистемы работают и взаимодействуют на одном или нескольких уровнях модели OSI.

Объекты сетевой подсистемы информационной инфраструктуры можно разделить на следующие группы [14]:

- оконечное оборудование (устройства субъектов цифровой среды, сервера, системы хранилищ данных);
- передающие устройства (коммуникационное оборудование);
- среда передачи.

Оконченное оборудование – устройство, которое генерирует сетевой трафик субъектов в процессе взаимодействия. К ним относятся стационарные и мобильные устройства, на которых запущенны приложения и сервисы.

Передающие устройства можно классифицировать по уровню эталонной модели взаимодействия открытых систем (модель OSI), на котором они работают [12]:

- физический уровень) – концентратор;
- (канальный) – коммутатор;
- (сетевой) – маршрутизатор, L3-коммутатор.

Каждое устройство выполняет задачи передачи данных и поддержки сетевого взаимодействия субъектов и объектов на своем уровне.

Среда передачи данных, реализуется посредством простых и составных каналов связи, использующих направляющие структуры трех основных типов:

- медные лини передачи (коаксиальный кабель, витая пара);
- оптические линии передачи (оптоволоконный кабель);
- беспроводная/радиоэфир (wi-fi, Bluetooth, NFC и т.д.).

Таким образом, процесс сетевого взаимодействия субъектов в информационной инфраструктуре можно описать кортежем (формула 1).

$$\langle S, R, P, C \rangle, \quad (1)$$

где S – множество субъектов (оконечных устройств) отправителей данных; R – множество субъектов (оконечных устройств) получателей данных; P- множество пакетов, циркулирующих от отправителя к получателю при сетевом взаимодействии; C – успешное или неуспешное (заблокированное) соединение отправителем и получателем, принимает значения согласно формуле 2.

$$C = \begin{matrix} established, \text{ соединение установлено} \\ not\ established, \text{соединение не установлено} \\ blocked, \text{соединение заблокировано} \end{matrix}. \quad (2)$$

Успешное соединение между узлами сети (состояние *established)* обеспечивает выполнение запросов и непрерывность бизнес-процессов объектов системы цифровой экономики. Блокировка соединения или сбои при установлении соединения указывают на проблемы сетевого взаимодействия, наиболее частыми причинами которых являются технические отказы оборудования [13], ошибки конфигурации [17] или успешная реализация угрозы информационной безопасности [10].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Инциденты безопасности

Под угрозой сетевой безопасности информационной инфраструктуры будет пониматься потенциально возможное сетевое событие, процесс или явление, которое посредством воздействия на данные (сетевой трафик) или объекты может прямо или косвенно привести к нанесению ущерба субъектов сетевого взаимодействия. Сетевая угроза безопасности в случае своего развития становится сетевой атакой, которая при успешной реализации приведет к вторжению и возникновению инцидента сетевой безопасности. Появление инцидента повышает вероятность реализации риска различного вида (см. рис. 3).

Согласно [20] инциденты не происходят по одному, а представляют поток одиночных, размножающихся и взаимодействующих инцидентов, которыми не всегда возможно сразу обнаружить и устранить, чем позже будет выявлен инцидент и приняты меры по его устранению, тем выше будет трудоемкость процесса (см. рис. 4).

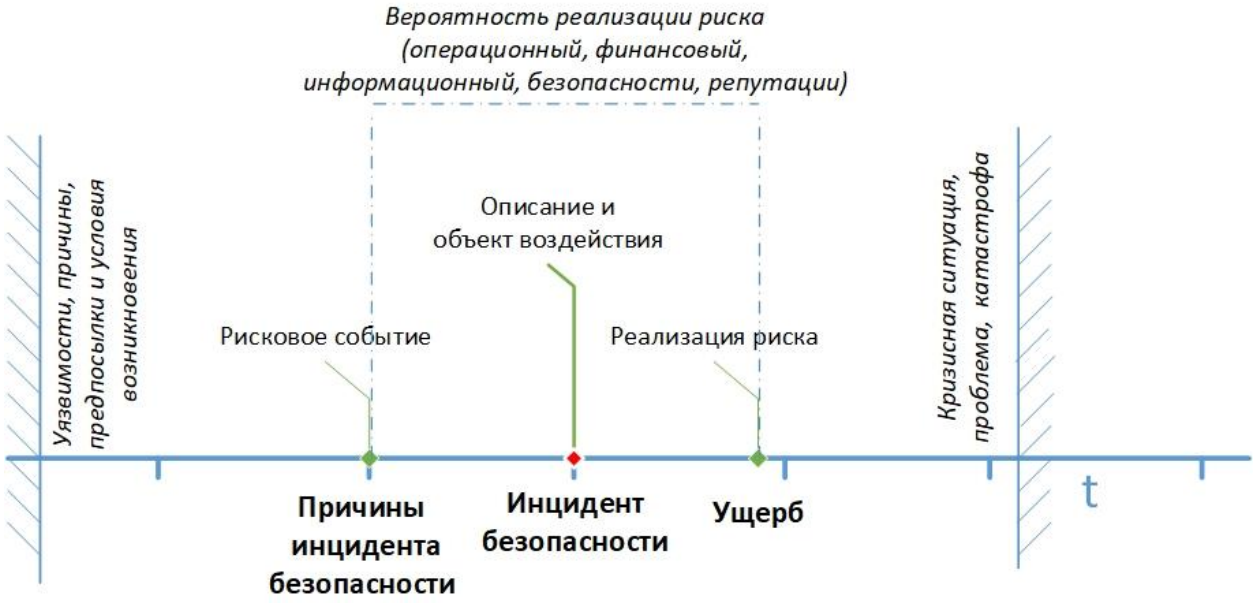

Рис. 3. Соотношение риска и инцидента безопасности
Fig.3. Ratio of risk and security incident

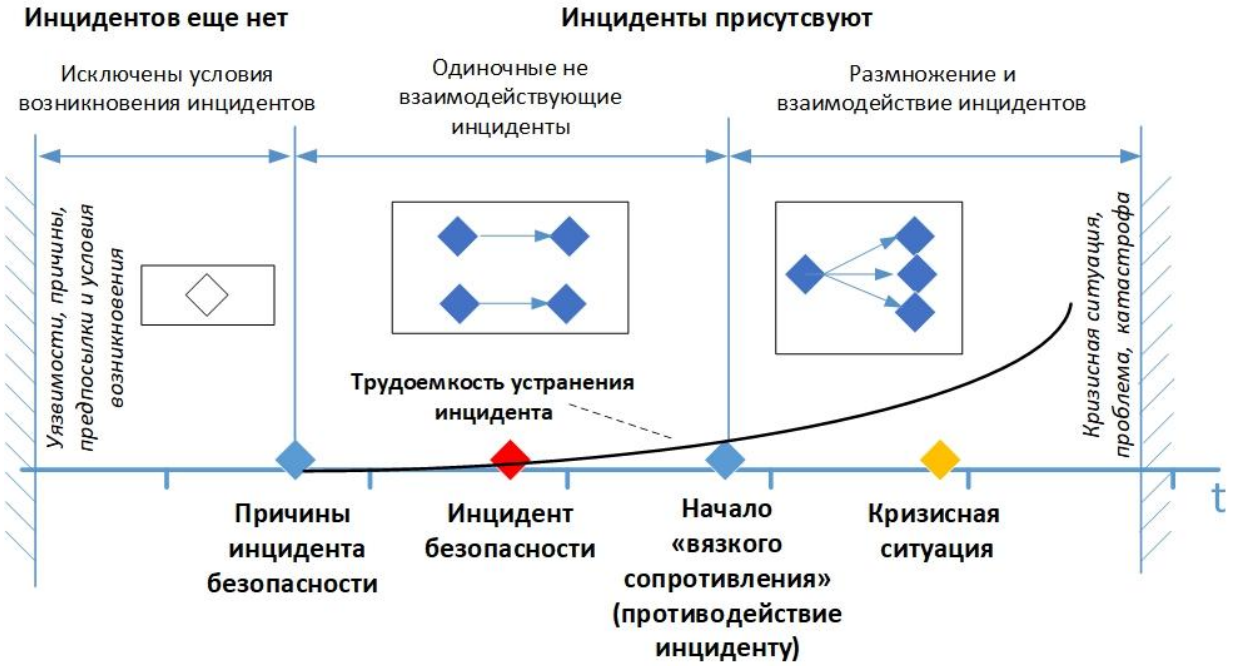

Рис. 4. Трудоемкость устранения инцидента безопасности на разных этапах жизненного цикла
Fig.4. Complexity of eliminating a security incident at different stages of the life cycle

Поэтому крайне важно выявлять предпосылки возникновения инцидентов и проводить комплекс мероприятий, которые исключают возникновение причин, порождающих инциденты, а это невозможно без решения задачи предварительной идентификации инцидента и его описания.

Разработка модели инцидентов сетевой безопасности

Таким образом, при построении описательной модели инцидентов сетевой безопасности необходимо выявить наиболее распространенные инциденты, анализ источников [3, 7, 11, 15] показывает, что основными видами инцидентов сетевой безопасности являются:

- реализация Dos/DDos-атак различного типа;
- использование специализированных вредоносных программ (вирусов, снифферов, троянских коней, почтовых червей, rootkit-ов и т.д.);
- сетевая разведка;
- IP-спуфинг;
- man-in-the-middle;
- инъекции (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция);
- phishing-атаки;
- отказ и повреждение технических и программных средств информационной инфраструктуры;
- повреждение каналов и линий связи.

Модель инцидентов позволяет выделить объект воздействия угрозы, описать возможные последствия и факторы, влияющие на вероятность ее реализации. В таблице представлена модель инцидентов сетевой безопасности для небольшой социотехнической системы цифровой экономки.

Таблица

Описание типовых инцидентов сетевой безопасности социотехнической системы

Table

Description of typical network security incidents of a socio-technical system

№	Наименование	Описание и объект воздействия	Последствия	Предпосылки и причины возникновения
1	Dos/DDos-атаки различного типа	генерация трафика для переполнения буфера и превышения допустимых пределов функционирования сети, блокирования сетевых служб Объекты: оконечные устройства, сетевое оборудование, сетевые службы	Прерывание бизнес-процессов, нарушение доступности данных и служб	Отсутствие фильтрации трафика, систем обнаружения и предотвращения вторжений
2	использование специализированных вредоносных программ	Заражение оконечных устройств и сетевого оборудования вредоносным ПО Объекты: оконечное оборудование и сетевые устройства	Утечка и нарушение целостности и доступности данных, нарушение непрерывности функционирования	Отсутствие антивирусных средств защиты,
3	сетевая разведка	несанкционированное сканирование и сбор информации о сети с помощью общедоступных данных и приложений. проводится в форме	утечка информации, сбор нарушителем данных для реализации целевой атаки	разрешенные ICMP запросы и эхо-ответ на периферийных маршрутизаторах. отсутствие

№	Наименование	Описание и объект воздействия	Последствия	Предпосылки и причины возникновения
		запросов DNS, эхо-тестирования и сканирования портов. Объекты: оконечные устройства, сетевое оборудование		межсетевого экранирования Не использование систем обнаружения вторжений
4	man-in-the-middle	Несанкционированное сканирование, перехват и анализ сетевого трафика, передаваемого между субъектами Объекты: транспортные протоколы и протоколы маршрутизации сетевого и оконечного оборудования	Утечка информации, получение несанкционированного доступа к частным сетевым ресурсам, искажение передаваемых данных и ввод несанкционированной информации в сетевые сессии	Отсутствие шифрования сетевого трафика
5	Инъекции	Несанкционированное внедрение специально сформированных сценариев и команд в код Объекты: базы данных, веб-приложения, оконечное оборудование	Утечка информации, нарушение доступности и целостности	Отсутствие контроля над выражениями и проверки вводимых данных, возможность несанкционированной загрузки файлов, уязвимости
6	phishing-атаки	процесс обмана или социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для несанкционированного использования Объекты: субъекты сетевого взаимодействия	Утечка информации	Отсутствие антивирусных средств, использование непроверенных ресурсов
7	IP-спуфинг	маскировка злоумышленника под санкционированного пользователя, ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между	утечка информации, подрыв доверия к субъектам сетевого взаимодействия	Отсутствие контроля доступа, криптографической аутентификации и фильтрации трафика

№	Наименование	Описание и объект воздействия	Последствия	Предпосылки и причины возникновения
		одноранговыми устройствами. Объекты: Таблицы маршрутизации, сетевое оборудование		
8	отказ и повреждение технических и программных средств информационной инфраструктуры	Нарушение работоспособности технических и программных средств, снижение показателей надежности Объекты: оконечное оборудование, сетевое оборудование	Прерывание бизнес-процессов, нарушение доступности данных и служб	Несвоевременное обслуживание и ремонт, отсутствие резервирования и избыточности
9	повреждение каналов и линий связи	Нарушение и блокирование процесса передачи информации, потеря данных Объекты: среда передачи	Прерывание бизнес-процессов, нарушение доступности данных и служб	Несвоевременное обслуживание и ремонт, отсутствие резервирования и избыточности

Каждый инцидент влечет операционные, финансовые, информационные и репутационные риски, обусловленные [18, 19]:

- возможностью удаленного администрирования и управления сетевым оборудованием и серверами;
- наличием круглосуточно доступных удаленных сервисов, баз данных и каналов обслуживания;
- использованием открытых, уязвимых сетевых протоколов передачи данных;
- небезопасной конфигурацией и ошибками в конфигурации объектов информационной инфраструктуры;
- регулярным доступом к услугам и сервисам множества субъектов;
- ростом числа уязвимостей программного обеспечения (системного, прикладного, в том числе и средств защиты) и использованием компонентов с известными уязвимостями;
- несвоевременным закрытием уязвимостей и обновлением программного-аппаратного обеспечения;
- небезопасной десериализацией данных и ошибками в коде сетевых сервисов и веб-приложений;
- слабыми паролями, утерей аутентификаторов, некорректной аутентификацией и управлением сессией;
- привязкой счетов карт и вкладов к интернет-банку и платежным сервисам;
- низкой информационной грамотностью или некомпетентностью некоторых категорий субъектов сетевого взаимодействия;
- незащищенным хранением личных данных субъектов сетевого взаимодействия;
- отсутствием некоторых подсистем защиты информации, например, контроля утечки информации, межсетевого экранирования, обнаружения атак и регистрации событий безопасности.

Реализуемые нарушителем угрозы могут проявляться в виде аномалий сетевого трафика определенного вида [2,16] и/или иметь явную сигнатуру и признаки сетевой атаки [4]. Для противодействия инцидентам и их последствиям необходимо использовать методы и средства обеспечения сетевой безопасности, в частности межсетевые экраны с глубоким анализом пакетов, системы обнаружения вторжения, антивирусные средства защиты. Источниками информации об рисковых событиях, составляющих сценарий развития инцидента безопасности являются журналы событий сетевых служб и сетевого оборудования, операционных систем, браузеров пользователей, средств защиты информации.

ЗАКЛЮЧЕНИЕ

Работая с потоком инцидентов безопасности, в динамичной социотехнической системе, важно уметь быстро обнаруживать инциденты, их идентифицировать, ранжировать и немедленно устранять срочные и опасные. Трудоемкость устранения инцидентов зависит от стадии жизненного цикла, на которой обнаружен инцидент, ведь чем раньше он будет обнаружен и локализован, тем меньшими последствиями и взаимодействием с другими инцидентами он будет обладать. Поэтому на этапе превентивных мер до начала «вязкого сопротивления инциденту» [1] нужно использовать описательные модели инцидентов и заполнять их карточки, что позволит более результативно проводить профилактику инцидентов и работать с ними в рамках системы управления.

В результате исследований были решены частные задачи:

- определены требования к безопасности и доверию в системе цифровой экономики Российской Федерации;
- проведен анализ типовой модели сетевого взаимодействия между объектами и субъектами в системе цифровой экономике;
- предложена описательная модель инцидентов сетевой безопасности.

Полученные в работе результаты могут быть использованы в рамках процедуры управления инцидентами, первыми этапами которой является идентификация инцидентов и их ранжирование по срочности и важности реакции на них:

- срочно устранять инцидент безопасности (высокий уровень риска);
- устранять инцидент безопасности в штатном режиме, постоянно проводя мониторинг состояния системы и контролирую последствия инцидента (средний уровень риска);
- отложить устранение инцидента, периодически контролируя его (средний низкий риска, приближенный к допустимому значению);
- игнорировать инцидент, принять сопутствующие ему риски (приемлемый риск).

Список литературы

1. Ананьин В. Сценарии управления инцидентами в разных моделях управления // Управляем предприятием. Особенности национального управления. М.: «Фирма 1 С». 2015 г. 41 с.

2. Бабенко А.А., Микова С.Ю., Оладько В.С. Разработка системы управления аномальными событиями информационной безопасности//Информационные системы и технологии. 2017. № 5 (103). С. 108-116.

3. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа: Лето, 2011. – С. 8-13. – URL https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 27.03.2019).

4. Гаврилова Е.А. Исследования методов обнаружения сетевых атак//Научные записки молодых исследователей. 2017. №4. С.55-58.

5. Горулев Д.А. Экономическая безопасность в условиях цифровой экономике // Технико-технологические проблемы сервиса. 2018. №3 (43). С. 77-83.

6. Ершова Т.В. Доверие и безопасность в цифровые экономики//Материалы форума Вольного экономического общества России «Цифровизация и национальная безопасность» (дата обращения: 06.03.2018).

7. Конарев И.И., Никишова А.В. Анализ методов обнаружения атак на WI-FI //В сборнике: Актуальные вопросы информационной безопасности регионов в условиях перехода России к цифровой экономике материалы VII Всероссийской научно-практической конференции. Волгоградский государственный университет. 2018. С. 28-32.

8. Логинов Е.Л., Райков А.Н. Цифровая экономика: уязвимость к сетевым атакам и возможности обеспечения устойчивости управления//Проблемы рыночной экономики. 2017. №4. С. 4-10.

9. Манахова И.В. Цифровое будущее и глобальная экономическая безопасность// Экономическая безопасность и качество. 2018. №1(30). С. 6-11.

10.Минзов А.С., Невский А.Ю., Баронов О.Ю. Информационная безопасность в цифровой экономике//ИТНОУ. 2018. №3. С.52-58.

11.Оладько В.С. Управление рисками непрерывности функционирования информационной инфраструктуры организации//Вестник компьютерных и информационных технологий. 2017. № 1(151). С. 44-56.

12.Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.

13.Петухов К. В., Стригунов Ю. В., Денисенко С. Е. Методы оценки надежности локальных вычислительных сетей. Разработка проекта локальной вычислительной сети / Под общей редакцией К.В. Петухова. – Темрюк, 2017. – 86 с.

14.Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.

15.Ananin E.V., Ananina I.S., Nikishova A.V. Examination of suspicious objects by virus analysts//Journal of Physics: Conference Series Сер. "International Conference Information Technologies in Business and Industry 2018 – Enterprise Information Systems" 2018. С. 042-042.

16.Ananin E.V., Nikishova A.V., Kozhevnikova I.S. Port scanning detection based on anomalies// 11th International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines", Dynamics 2017 Proceedings. 2017. С. 1-5.

17.Boughton N. Protecting the world of connected devices// Network Security Volume 2019, Issue 6, June 2019, Pages 11-13 doi: https://doi.org/10.1016/S1353-4858(19)30072-8

18.Herbert S. Why IIoT should make businesses rethink security// Network Security Volume 2019, Issue 7, July 2019, Pages 9-11. Doi: https://doi.org/10.1016/S1353-4858(19)30083-2

19.Oladko V.S. Cybersecurity issues in the implementation of the digital economy// Sochi Journal of Economy. 2018. Т. 12. № 1. С. 68-78.

20.Enterprise Risk Management – Integrated Framework. Executive Summary, 2004, Committee of Sponsoring Organizations of the Treadway Commission (COSO), AICPA.

References

1. Ananyin V. (2015), Scenarios of incident management in different management models, We manage the enterprise. Features of national governance. M .: "Firm 1 S", 4.

2. Babenko A.A., Mikova S.Yu., Oladko V.S., (2017), Development of a system for managing abnormal events of information security, Information Systems and Technologies, 5 (103), 108-116.

3. Borshevnikov A.E. (2011), Network attacks. Kinds. Ways of struggle, Modern trends in technical sciences: materials of Intern. scientific conf. (Ufa, October 2011), 8-13. URL https://moluch.ru/conf/tech/archive/5/1115/ (accessed: 03/27/2019).

4. Gavrilova E.A. (2017), Investigations of network attack detection methods, Scientific notes of young researchers, 4, 55-58.

5. Gorulev D.A. (2018), Economic security in the digital economy, Technical and technological problems of service, 3 (43), 77-83.

6. Ershova T.V. (2018), Trust and security in the digital economy, Materials of the forum of the Free Economic Society of Russia “Digitalization and National Security”.

7. Konarev I.I., Nikishova A.V. (2018), Analysis of methods for detecting attacks on WI-FI, Actual issues of information security of regions in the context of Russia's transition to a digital economy, materials of the VII All-Russian Scientific and Practical Conference. Volgograd State University, 28-32.

8. Loginov E.L., Raikov A.N. (2017), Digital economy: vulnerability to network attacks and the possibility of ensuring the sustainability of management, Problems of a market economy, 4, 4-10.

9. Manakhova I.V. (2018), Digital future and global economic security, Economic security and quality, 1 (30), 6 – 11.

10.Minzov A.S., Nevsky A.Yu., Baronov O.Yu. (2018), Information Security in the Digital Economy, ITNOU, 3, 52 – 58.

11.Oladko V. S. (2017), Risk management continuity of information infrastructure in the organization, Vestnik komp'yuternykh i informatsionnykh tekhnologiy, 1 (151), 44-56.DOI: 10.14489/vkit.2017.01. pp. 044-052

12.Olifer V., Olifer N. (2016), Computer networks. Principles, technologies, protocols: Textbook for universities. 5th ed. – St. Petersburg: Peter, 992.

13.Petukhov K.V., Strigunov Yu. V., Denisenko S.E. (2017), Methods for assessing the reliability of local area networks. Development of a local area network project, Under the general editorship of K.V. Petukhov. – Temryuk, 86.

14.Tanenbaum E., Weatheroll D. (2012), Computer networks. 5th ed. – St. Petersburg: Peter, 960.

15.Ananin E.V., Ananina I.S., Nikishova A.V. (2018), Examination of suspicious objects by virus analysts, Journal of Physics: Conference Series Cep. "International Conference Information Technologies in Business and Industry 2018 – Enterprise Information Systems", 042-042.

16.Ananin E.V., Nikishova A.V., Kozhevnikova I.S. (2017), Port scanning detection based on anomalies, 11th International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines", Dynamics 2017 Proceedings, 1-5.

17.Boughton N. (2019), Protecting the world of connected devices, Network Security, 6, 11-13 doi: https://doi.org/10.1016/S1353-4858(19)30072-8

18.Herbert S. (2019), Why IIoT should make businesses rethink security, Network Security, 7, 9-11, doi: https://doi.org/10.1016/S1353-4858(19)30083-2

19.Oladko V.S. (2018), Cybersecurity issues in the implementation of the digital economy, Sochi Journal of Economy, 1(12), 68-78.

20.Enterprise Risk Management – Integrated Framework. Executive Summary, (2004), Committee of Sponsoring Organizations of the Treadway Commission (COSO), AICPA.

Оладько Владлена Сергеевна, кандидат технических наук, доцент кафедры информационной безопасности

Oladko Vladlena Sergeevna, Candidate of Technical Sciences, Assistant Professor of the Information Security Department