Учредитель

ФГБОУ ВО «Новосибирский государственный технический университет»

Редакционный совет

Председатель редакционного совета

Вострецов Алексей Геннадьевич, д-р техн. наук, проф., засл. деятель науки РФ, НГТУ, г. Новосибирск

Заместители председателя

Белим Сергей Викторович, д-р физ.-мат. наук, проф., ОмГТУ, г. Омск
Белов Виктор Матвеевич, д-р техн. наук, проф., НГТУ, г. Новосибирск
Котенко Игорь Витальевич, д-р техн. наук, проф., СПИИРАН, г. Санкт-Петербург

Члены редакционного совета

Авдеенко Татьяна Владимировна, д-р техн. наук, проф., НГТУ, г. Новосибирск
Аверченков Владимир Иванович, д-р техн. наук, проф., Брянский ГТУ, г. Брянск
Алгулиев Расим Магомед оглу, д-р техн. наук, проф., академик НАН Республики Азербайджан, ИИТ НАН Республики Азербайджан, г. Баку
Аникин Игорь Вячеславович, д-р техн. наук, доцент, КНИТУ-КАИ, г. Казань
Арутюнян Мариам Евгеньевна, д-р физ.-мат. наук, проф., ИИиАП НАН Республики Армения, г. Ереван
Баранкова Инна Ильинична, д-р техн. наук, доцент, МГТУ им. Г.И. Носова, г. Магнитогорск
Беззатеев Сергей Валентинович, д-р техн. наук, доцент, СПбГУАП, г. Санкт-Петербург
Боранбаев Сейлхан Нарбутинович, д-р техн. наук, проф., Евразийский национальный университет им. Л.Н. Гумилева, г. Нур-Султан, Республика Казахстан
Васильев Владимир Иванович, д-р техн. наук, проф., УГАТУ, г. Уфа
Воевода Александр Александрович, д-р техн. наук, проф., НГТУ, г. Новосибирск
Гатчин Юрий Арменакович, д-р техн. наук, проф., ИТМО, г. Санкт-Петербург
Громов Юрий Юрьевич, д-р техн. наук, проф., Тамбовский ГТУ, г. Тамбов
Иващук Ольга Александровна, д-р техн. наук, проф., НИУ «БелГУ», г. Белгород
Киселёва Тамара Васильевна, д-р техн. наук, проф., СибГИУ, г. Новокузнецк
Кулаков Станислав Матвеевич, д-р техн. наук, проф., СибГИУ, г. Новокузнецк
Кульба Владимир Васильевич, д-р техн. наук, проф., ИПУ РАН, г. Москва
Кытманов Алексей Александрович, д-р физ.-мат. наук, доцент, СФУ, г. Красноярск
Лавлинский Сергей Михайлович, д-р техн. наук, доцент, Институт математики им. С.Л. Соболева СО РАН, г. Новосибирск
Ленский Артем, PhD, ст. науч. сотр., Австралийский национальный университет, г. Канберра
Магазев Алексей Анатольевич, д-р физ.-мат. наук, проф., ОмГТУ, г. Омск
Макарова Елена Анатольевна, д-р техн. наук, проф., УГАТУ, г. Уфа
Митрохин Валерий Евгеньевич, д-р техн. наук, проф., ОмГУПС, г. Омск
Мышляев Леонид Павлович, д-р техн. наук, проф., СибГИУ, г. Новокузнецк
Пагано Микеле, д-р, проф., Пизанский университет, г. Пиза, Италия

Пиотровский Дмитрий Леонидович, д-р техн. наук, проф., Средиземноморский Карпасский университет, Турецкая Республика Северного Кипра
Петрунин Юрий Юрьевич, д-р филос. наук, проф., МГУ им. М.В. Ломоносова, г. Москва
Тузиков Александр Васильевич, д-р физ.-мат. наук, проф., чл.-корр. НАН Республики Беларусь, ОИПИ НАН Республики Беларусь, г. Минск
Харин Юрий Семенович, д-р физ.-мат. наук, проф., чл.-корр. НАН Республики Беларусь, БГУ, г. Минск
Ходашинский Илья Александрович, д-р техн. наук, проф., ТУСУР, г. Томск
Шарипов Бахыт Жапарович, д-р пед. наук, проф., Международный университет информационных технологий, г. Алматы, Республика Казахстан
Ячиков Игорь Михайлович, д-р техн. наук, проф., МГТУ им. Г.И. Носова, г. Магнитогорск

Редакция

Главный редактор

Вострецов Алексей Геннадьевич, д-р техн. наук, проф., засл. деятель науки РФ, НГТУ, г. Новосибирск

Заместитель главного редактора

Белов Виктор Матвеевич, д-р техн. наук, проф., НГТУ, г. Новосибирск

Журнал зарегистрирован 01.03.2021 Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации ПИ № ФС 77-80320

Адрес издателя и редакции: 630073, г. Новосибирск, пр. К. Маркса, 20.
E-mail: office@publish.nstu.ru и digital-tech-security@mail.ru
Web site: http://publish.nstu.ru и http://journals.nstu.ru/digital-tech-security/

Publisher and editorial office adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Fe-deration

До номера 1 (100) 2021 г. включительно журнал выходил под названием «Сборник научных трудов НГТУ» (ISSN 2307-6879)

16+

© Коллектив авторов, 2023
© Новосибирский государственный технический университет, 2023

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ

ISSN 2782-2230

№ 4 (111) **2023**

СОДЕРЖАНИЕ

Выпускающий редактор *И.П. Бровановa*
Корректор *Л.Н. Киншт*
Компьютерная верстка *С.И. Ткачева*

Лицензия № ИД 04303 от 20.03.01. Подписано в печать 20.12.2023. Выход в свет 25.12.2023
Формат 60×84/16. Бумага офсетная. Тираж 300 экз. Уч.-изд. л. 5,11
Печ. л. 5,5. Изд. № 246. Заказ № 327. Цена свободная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20

Editorial board

Novosibirsk State Technical University

Editorial council

Chairman of the editorial council

Vostretsov A.G., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF

Deputy chairman

Belim S.V., Dr. Sc. (Phys. & Math.), Omsk State Technical University, Omsk, RF
Belov V.M., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF
Kotenko I.V., Dr. Sc. (Eng.), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, RF

The members of the editorial council

Avdeenko T.V., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF
Averchenkov V.I., Dr. Sc. (Eng.), Bryansk State Technical University, Bryansk, RF
Alguliyev R.M.o., Dr. Sc. (Eng.), Azerbaijan National Academy of Sciences, Institute of Information Technology, Baku, AZE
Anikin I.V., Dr. Sc. (Eng.), Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, RF
Haroutunian M.E., Dr. Sc. (Phys. & Math.), Institute for Informatics and Automation Problems of NAS RA, Yerevan, ARM
Barankova I.I., Dr. Sc. (Eng.), Nosov Magnitogorsk State Technical University, Magnitogorsk, RF
Bezzateev S.V., Dr. Sc. (Eng.), Saint Petersburg State University of Aerospace Instrumentation, St. Petersburg, RF
Boranbaev S.N., Dr. Sc. (Eng.), L.N. Gumilyov Eurasian National University, Nur-Sultan, KZ
Vasil'ev V.I., Dr. Sc. (Eng.), Ufa State Aviation Technical University, UFA, RF
Voevoda A.A., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF
Gatchin Yu.A., Dr. Sc. (Eng.), National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, RF
Gromov Yu.Yu., Dr. Sc. (Eng.), Tambov State Technical University, Tambov, RF
Ivashhuk O.A., Dr. Sc. (Eng.), Belgorod State National Research University, Belgorod, RF
Kiseljova T.V., Dr. Sc. (Eng.), Siberian State Industrial University, Novokuznetsk, RF
Kulakov S.M., Dr. Sc. (Eng.), Siberian State Industrial University, Novokuznetsk, RF
Kul'ba V.V., Dr. Sc. (Eng.), V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, RF
Kytmanov A.A., Dr. Sc. (Phys. & Math.), Siberian Federal University, Krasnoyarsk, RF
Lavlinskij S.M., Dr. Sc. (Eng.), Sobolev Institute of Mathematics of Russian Academy of Sciences, Novosibirsk, RF
Lenskij A., PhD, Australian National University, Canberra, AUS
Magazev A.A., Dr. Sc. (Phys. & Math.), Omsk State Technical University, Omsk, RF
Makarova E.A., Dr. Sc. (Eng.), Ufa State Aviation Technical University, Ufa, RF

Mitrokhin V.E., Dr. Sc. (Eng.), Omsk State Transport University, Omsk, RF
Myshljaev L.P., Dr. Sc. (Eng.), Siberian State Industrial University, Novokuznetsk, RF
Pagano M., Dr. Sc., University of Pisa, Pisa, IT
Piotrovskij D.L., Dr. Sc. (Eng.), University of Mediterranean Karpasia, Turkish Republic of Northern Cyprus, CYP
Petrunin Yu.Yu., Dr. Sc. (Philos.), Lomonosov Moscow State University, Moscow, RF
Tuzikov A.V., Corresponding Member, National Academy of Sciences of Republic Belarus, Dr. Sc. (Phys. & Math.), United Institute of Informatics Problems, Minsk, BLR
Harin Yu.S., Corresponding Member, National Academy of Sciences of Republic Belarus, Dr. Sc. (Phys. & Math.), Belarusian State University, Minsk, BLR
Hodashinskij I.A., Dr. Sc. (Eng.), Tomsk State University of Control Systems and Radioelectronics, Tomsk, RF
Sharipov B.Zh., Dr. Sc. (Ped.), International University of Information Technology, Almaty, KZ
Jachikov I.M., Dr. Sc. (Eng.), Nosov Magnitogorsk State Technical University, Magnitogorsk, RF

Editorial office

Chief editor

Vostretsov A.G., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF

Deputy chief editor

Belov V.M., Dr. Sc. (Eng.), Novosibirsk State Technical University, Novosibirsk, RF

Publisher and editorial adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation
E-mail: office@publish.nstu.ru, digital-tech-security@mail.ru
Web site: http://publish.nstu.ru, http://journals.nstu.ru/digital-tech-security/

© Authors, 2023
© Novosibirsk State Technical University, 2023

DIGITAL TECHNOLOGY SECURITY

ISSN 2782-2230

№ 4 (111) **2023**

CONTENTS

Publishing Editor *I.P. Brovanova*
Editor *L.N. Kinsht*
Computer imposition *S.I. Tkacheva*

License № ID 04303 from 20.03.01. Signed in print December 20, 2023
Date of publication December 25, 2023. Format 60 × 84 1/16
Offset Paper. Circulation is 300 copies. Educational-ed. liter. 5,11. printed pages 5,5
Publishing number 246. Order number 327

It is printed in printing house of Novosibirsk State Technical University
630073, Novosibirsk, 20 K. Marx Prospekt

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111). – 9–23

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

УДК 004.056 DOI: 10.17212/2782-2230-2023-4-9-23

МЕТОДИКА ОРГАНИЗАЦИИ ПРОЦЕССА МОНИТОРИНГА РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ*

А.В. ИВАНОВ[1], И.А. ОГНЕВ[2], И.В. НИКРОШКИН[3], Ю.А. ПОПОВА[4]

[1] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, старший научный сотрудник лаборатории искусственного интеллекта и информационных технологий. E-mail: andrej.ivanov@corp.nstu.ru*

[2] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: i.ognev.2016@corp.nstu.ru*

[3] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: i.nikroshkin@corp.nstu.ru*

[4] *630073, РФ, г. Новосибирск, пр. К. Маркса, 20, Новосибирский государственный технический университет, лаборант инжинирингового центра «Информационная безопасность». E-mail: yu.popova.2019@stud.nstu.ru*

Статья посвящена методике организации процесса мониторинга распределенных информационных систем. Рассмотрена общая концепция построения процесса мониторинга информационной безопасности. Особое внимание уделено таким недостаткам распределенных систем, как проблемы администрирования системы, проблемы ограниченности масштабируемости распределенных систем и проблемы переносимости программного обеспечения. Был сделан вывод о том, что в настоящее время нет единого подхода для устранения указанных недостатков при построении процесса мониторинга. Приведена модель децентрализованной распределенной системы, для которой разработана методика организации процесса мониторинга. Описано три подхода к организации процесса мониторинга распределенных информационных систем, а именно: организация мониторинга сетевой активности информационной системы, организация мониторинга хостовой активности информационной системы и смешанный подход. В методике используется смешанный подход, основанный на мониторинге сетевой и хостовой активности. Рассмотрен процесс приоритизации источников событий информационной безопасности, который включает в себя оценку рисков

* Статья получена 10 ноября 2023 г.

ИБ, выявление актуальных угроз ИБ и критичных активов организации. В результате предложена методика организации процесса мониторинга распределенных информационных систем, состоящая из четырех этапов: расчета рисков, определения актуальных угроз, приоритизации источников событий информационной безопасности и подключения выбранных источников к системе мониторинга событий информационной безопасности.

Ключевые слова: информационная безопасность, кибербезопасность, мониторинг, распределенные информационные системы, центр мониторинга, SOC, события информационной безопасности, инциденты информационной безопасности

ВВЕДЕНИЕ

Многие организации принимают во внимание современные угрозы информационной безопасности из-за постоянных компьютерных атак. Злоумышленники могут находиться в сети компании до 15 дней [1], прежде чем их обнаружат, что приводит к финансовым потерям. В 2018 году крупные компании пострадали от атаки вируса-шифровальщика. В прошлом году случаи утечки конфиденциальной информации и шпионажа увеличились, и этот год не исключение. Поиск решений для минимизации таких рисков сейчас очень актуален.

Построение Security Operation Center (SOC), который объединяет программное обеспечение, аппаратное обеспечение, персонал и процессы, является эффективным решением для обеспечения информационной безопасности [2, 3]. SOC предназначен для централизованного сбора и анализа информации об инцидентах информационной безопасности, поступающей из различных источников ИТ-инфраструктуры. Этот подход является ключевым компонентом в обеспечении информационной безопасности организации, поскольку он направлен на мониторинг, обнаружение и оперативную реакцию на инциденты, что в результате способствует снижению возможных негативных последствий.

Работа выполнена в рамках государственного задания ИВМиМГ СО РАН № 0251-2022-0005.

1. ФОРМИРОВАНИЕ ПРОБЛЕМАТИКИ

Построение SOC в сфере информационной безопасности является одной из наиболее популярных тем на сегодняшний день [4]. Существует множество работ, содержащих руководство по выстраиванию процессов мониторинга информационной безопасности, интеграции программных решений и выбору источников событий для выявления компьютерных атак и инцидентов ин-

формационной безопасности [5–7]. Общая концепция структурно выглядит следующим образом:

1) планирование;
2) проектирование;
3) строительство;
4) управление;
5) рефлексия.

Информационные системы можно разделить по географическому признаку на распределенные и нераспределенные. В нераспределенных информационных системах и централизованных распределенных системах процесс выстраивания мониторинга достаточно проработан в силу относительной простоты, так как в нераспределенной системе вся информация находится в ведении одной внутренней структуры, а в централизованной распределенной системе все ее сегменты построены по одинаковому принципу. Более сложная задача – выстроить эффективный процесс мониторинга в децентрализованной распределенной системе, разными частями которой заведуют разные подразделения в условиях отсутствия общих требований в построении и администрировании сетей.

Распределенные системы имеют свои особенности:

- проблемы администрирования, включая балансирование нагрузки и восстановление данных при ошибках;
- ограничения масштабируемости;
- проблемы переносимости программного обеспечения.

Основные проблемы администрирования в распределенных системах:

- балансировка нагрузки на узлы системы;
- восстановление данных при ошибке;
- сбор статистики с узлов системы;
- автоматическое обновление программного обеспечения на узлах системы.

Ограничения масштабируемости – это действительно одна из ключевых проблем при проектировании распределенных систем. Распределенные системы помогли избежать ограничений возможности увеличения вычислительной мощности. Существует три основных показателя масштабируемости системы [8]:

- масштабируемость относительно размера, что позволяет простое подключение новых узлов;
- географическая масштабируемость, позволяющая подключать новые узлы к сети без привязки к конкретной географической зоне;

• масштабируемость управления, означающая, что администрирование системы не становится более сложным при увеличении общего количества узлов.

Проблема переносимости программного обеспечения действительно ограничивает развитие и расширение распределенных систем. Быстрое развитие программных архитектур, языков программирования и ИТ-индустрии в целом требует разработки методологий для обеспечения переносимости программного кода.

В области мониторинга информационной безопасности актуальными проблемами распределенных систем являются проблемы администрирования, переносимости ПО, а также прозрачности системы [9]. Под прозрачностью системы будем понимать восприятие системы как однородного объекта, а не набора автономных сервисов. Решение данных проблем связано с уровнями стратегии построения SOC.

Если проблемы на 3-м и 4-м этапе решены силами вендоров систем мониторинга событий информационной безопасности [10–12], то для решения проблем на 1-м и 2-м этапе нет единого подхода.

2. ОСНОВНЫЕ ЭЛЕМЕНТЫ МЕТОДИКИ

2.1. РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ

Распределенные системы можно представить как неполносвязный граф [13] (рис. 1).

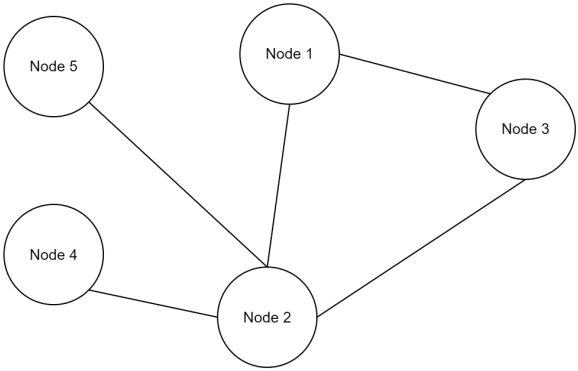

Рис. 1. Модель распределенной системы

Fig. 1. Distributed System Model

Однако в то время как в [13] распределенная система рассматривается как совокупность вычислительных узлов, в нашем случае необходимо рассматривать распределенную систему как совокупность самостоятельных систем (рис. 2).

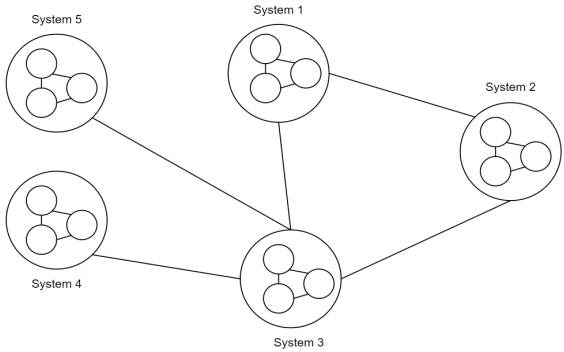

Рис. 2. Распределенная система как совокупность систем

Fig. 2. Distributed system as a set of systems

При рассмотрении такой модели будем считать, что каждая отдельная система строится по заранее заданному шаблону организацией, при этом состав систем и связи внутри системы похожи друг на друга. Обратим внимание на более сложный случай – децентрализованную распределенную систему (рис. 3). Децентрализованная распределенная система – распределенная система, в которой каждый узел-система имеет уникальный состав и внутренние связи.

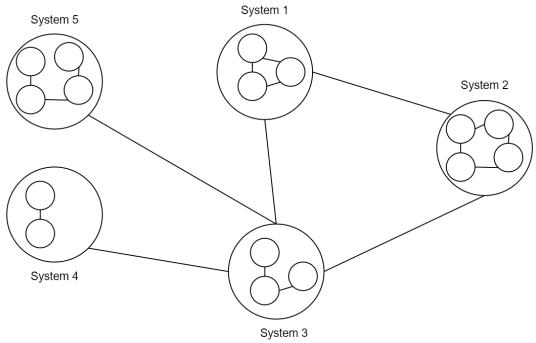

Рис. 3. Децентрализованная распределенная система

Fig. 3. Decentralized Distributed System

Далее под распределенной системой будем подразумевать децентрализованную распределенную систему (рис. 3) как самый сложный случай для построения процесса мониторинга событий информационной безопасности.

2.2. ПОДХОДЫ К ОРГАНИЗАЦИИ ПРОЦЕССА МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

К вопросу организации процесса мониторинга информационных систем можно подойти с помощью трех подходов:

1) организации мониторинга сетевой активности информационной системы [14, 15];

2) организации мониторинга хостовой активности информационной системы [16, 17];

3) смешанного подхода, основанного на мониторинге сетевой и хостовой активности [18, 19].

Рассматривая первый случай, можно выделить достоинство в том, что зачастую мониторинг организуется сбором событий информационной безопасности с физической или логической границы сети – это позволяет упростить интеграцию системы мониторинга событий информационной безопасности в любые распределенные и нераспределенные системы. Однако данный подход имеет довольно большой недостаток: при мониторинге создается неполная картина активности информационной системы.

Второй случай также не лишен недостатка – ограниченности видимости активности внутри информационной системы. Однако помимо этого недостатка имеется еще один – сложность интеграции в децентрализованные распределенные информационные системы, так как не удается создать единый подход к выбору и подключению источников событий информационной безопасности.

Третий случай, с одной стороны, объединяет все недостатки предыдущих двух подходов, однако имеет одно главное преимущество: одновременный анализ сетевой и хостовой активности позволяет создать полную видимость активности внутри информационной системы и прозрачность каждого узла-системы для службы информационной безопасности и, как следствие, для ИТ-служб.

В нашей работе будет использоваться смешанный подход к построению процесса мониторинга событий информационной безопасности децентрализованных распределенных информационных систем, однако предстоит найти решение для преодоления недостатка, касающегося большой сложности вы-

бора источников событий информационной безопасности в силу уникальности каждого узла-системы. Эта проблема решается использованием инвентаризации и последующей приоритизацией потенциальных источников событий информационной безопасности.

2.3. ПРИОРИТИЗАЦИЯ ИСТОЧНИКОВ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Приоритизация источников событий информационной безопасности является одним из следствий, которое можно извлечь из процесса управления рисками. Управление рисками – процесс, заключающийся в выявлении, идентификации и оценке рисков ИБ, которые могут привести к недопустимым событиям и (или) невыполнению бизнес-целей организации [20].

Результат процесса управления рисками – список рисков ИБ, актуальных для организации. Этот список рисков можно переложить в плоскость актуальных угроз ИБ [21]. Модель угроз содержит в себе модели нарушителя, а также возможные векторы компьютерной атаки на информационную систему [21, 22].

Таким образом, приоритизация источников событий информационной безопасности выглядит следующим образом:

1) оценка рисков ИБ;
2) выявление актуальных угроз ИБ;
3) выявление критичных активов, которые могут быть подвержены компьютерным атакам или могут содержать в себе следы компрометации компьютерного инцидента.

3. МЕТОДИКА ОРГАНИЗАЦИИ ПРОЦЕССА МОНИТОРИНГА РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Для организации эффективного процесса мониторинга распределенных информационных систем необходимо подключить к системе мониторинга критичные активы и активы, которые могут свидетельствовать о компрометации любого сегмента информационной системы. Для процесса мониторинга используется модель подключения сетевых и хостовых источников событий информационной безопасности.

1. Расчет рисков.

Для расчета рисков ИБ необходимо определить следующие сущности:

– основные и вспомогательные бизнес-процессы организации;
– распределение бизнес-процессов по распределенным сегментам информационной системы;

– выявление недопустимых событий организации;

– определение защищаемых активов в соответствии с требованиями федеральных органов исполнительной власти, ответственных за обеспечение безопасности государственных информационных систем, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами, критической информационной инфраструктуры Российской Федерации.

Далее необходимо оценить критичность выявленных бизнес-процессов – выполнить оценку экономических, репутационных потерь при нарушении нормальной деятельности бизнес-процесса.

2. Определение актуальных угроз.

Необходимо выявить актуальные угрозы ИБ, которые могут привести к реализации недопустимых событий, выявить актуальных нарушителей и возможные векторы реализации компьютерных атак. Такую деятельность необходимо провести в каждом сегменте распределенной информационной системы.

3. Приоритизация источников событий информационной безопасности.

Исходя из векторов возможных компьютерных атак выявить критические системы, непрерывность деятельности которых может привести к недопустимым событиям для организации. Чем выше возможный ущерб для организации, тем выше приоритет у целевого актива.

Для каждого сегмента распределенной системы необходимо составить свой список.

4. Подключение выбранных источников к системе мониторинга событий информационной безопасности.

Используя функционал современных систем мониторинга событий информационной безопасности, необходимо разместить в каждом сегменте сети сборщика (коллектор, агент) событий информационной безопасности. Для обеспечения связи с единым центром обработки событий информационной безопасности каждый сборщик должен передавать события информационной безопасности по защищенному каналу передачи информации.

Каждый сегмент распределенной системы должен обеспечить непрерывную или близкую к непрерывной передачу событий информационной безопасности.

Итого, каждый сегмент распределенной информационной системы должен быть полностью изучен, и должны быть выявлены критические активы, за которыми необходим постоянный мониторинг их безопасности. Подключение всех критичных активов в централизованный центр обработки событий информационной безопасности позволит обеспечить прозрачность каждого

сегмента информационной системы и обеспечить централизацию управления событиями информационной безопасности.

ЗАКЛЮЧЕНИЕ

В настоящее время отсутствует единый подход для решения проблем, которые возникают при построении процесса мониторинга информационной безопасности распределенных систем. В связи с этим была разработана методика, которая позволяет решить проблемы администрирования системы и переносимости программного обеспечения. Разработанная методика включает в себя четыре этапа.

1. Расчет рисков – классификация основных и вспомогательных бизнес-процессов по распределенным сегментам ИС и выявление недопустимых событий для определения критичных ИТ-активов.

2. Определение актуальных угроз – выявление актуальных угроз ИБ, нарушителей и векторов реализации атак в каждом сегменте ИС.

3. Приоритизация источников событий информационной безопасности – составление списка критичных активов, для которых необходим постоянный мониторинг безопасности.

4. Подключение выбранных источников к системе мониторинга событий информационной безопасности – обеспечение непрерывной передачи событий ИБ в каждом сегменте распределенной ИС.

СПИСОК ЛИТЕРАТУРЫ

1. По данным Sophos, время пребывания злоумышленников в сети увеличилось на 36 % // SecurityLab.ru. – 2022, 9 июня. – URL: https://www.securitylab.ru/finance_news/532207 (дата обращения: 01.12.2023).

2. *Стрельников Р.В.* SOC. Неэффективность внедрения // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. – 2019. – № 4. – С. 81–85.

3. *Muniz J., McIntyre G., AlFardan N.* Security operations center: building, operating, and maintaining your SOC. – Cisco Press, 2015. – URL: http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052076 (accessed: 01.12.2023).

4. Создание и управление Security Operations Center для эффективного применения в реальных условиях / А.А. Казанцев, А.В. Красов, А.И. Катасонов, А.М. Гельфанд // Актуальные проблемы инфотелекоммуникаций

в науке и образовании: VIII Международная научно-техническая и научно-методическая конференция. – СПб.: СПбГУТ, 2019. – С. 590–595.

5. *Mughal A.A.* Building and securing the modern Security Operations Center (SOC) // International Journal of Business Intelligence and Big Data Analytics. – 2022. – Vol. 5 (1). – P. 1–15.

6. *Alahmadi B.A., Axon L., Martinovic I.* 99 % false positives: a qualitative study of SOC analysts' perspectives on security alarms // 31st USENIX Security Symposium. – Boston: USENIX Association, 2022. – P. 2783–2800.

7. *Shahjee D., Ware N.* Integrated network and Security Operation Center: a systematic analysis // IEEE Access. – 2022. – Vol. 10. – P. 27881–27898.

8. *Таненбаум Э., Стеен М. ван.* Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 876 с.

9. *Цветков В.Я., Алпатов А.Н.* Проблемы распределенных систем // Перспективы науки и образования. – 2014. – № 6 (12). – С. 31–36.

10. Об установке конвейеров обработки событий // Positive Technologies. Документация по продуктам. – URL: https://help.ptsecurity.com/projects/siem/latest/ru-RU/help/3690716683 (дата обращения: 01.11.2023).

11. KOMRAD Enterprise SIEM // Эшелон. Комплексная безопасность. – URL: https://npo-echelon.ru/production/65/11793 (дата обращения: 01.11.2023).

12. RuSIEM. – URL: https://rusiem.com/ru/products/rusiem (дата обращения: 01.11.2023).

13. *Дурнов Р.В.* Модель распределенной вычислительной сети // Известия ТулГУ. Технические науки. – 2022. – № 9. – С. 151–153.

14. *Дудникова А.И.* Разработка системы мониторинга сетевого трафика на базе Flow-протоколов // Молодежь. Общество. Современная наука, техника и инновации. – 2021. – № 20. – С. 193–195. – Яз. англ.

15. *Kim S., Park K.-J., Lu C.* A survey on network security for cyber–physical systems: from threats to resilient design // IEEE Communications Surveys & Tutorials. – 2022. – Vol. 24 (3). – P. 1534–1573. – DOI: 10.1109/COMST.2022.3187531.

16. Host-based IDS: a review and open issues of an anomaly detection system in IoT / I. Martins, J.S. Resende, P.R. Sousa, S. Silva, L. Antunes, J. Gama // Future Generation Computer Systems. – 2022. – Vol. 133. – P. 95–113.

17. *Formby D., Beyah R.* Temporal execution behavior for host anomaly detection in programmable logic controllers // IEEE Transactions in Information Forensics and Security. – 2020. – Vol. 15. –P. 1455–1469.

18. *Skendžić A., Kovačić B., Balon B.* Management and monitoring security events in a business organization – SIEM system // 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO). – Opatija: IEEE, 2022. – P. 1203–1208.

19. *Thursday Ehis A.-m.* Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture // Archives of Advanced Engineering Science. – 2023. – P. 1–10. – DOI: 10.47852/bonviewAAES32021068.

20. *Бирюков С.А., Дьяков С.А.* Применение методики управления рисками в малых и средних строительных организациях // Вестник Академии знаний. – 2021. – № 42 (1). – С. 36–45.

21. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix / W. Xiong, E. Legrand, O. Åberg, R. Lagerström // Software and Systems Modeling. – 2022. – Vol. 21 (1). – P. 157–177. – DOI: 10.1007/s10270-021-00898-7.

22. Методический документ «Методика оценки угроз безопасности информации» от 5 февраля 2021 г. (с изм. и доп. в ред. от 06.12.2022). – ФСТЭК России, 2021.

Иванов Андрей Валерьевич, старший научный сотрудник лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук. E-mail: andrej.ivanov@corp.nstu.ru

Огнев Игорь Александрович, инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук. E-mail: i.ognev.2016@corp.nstu.ru

Никрошкин Иван Владимирович, инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики Сибирского отделения Российской академии наук. E-mail: i.nikroshkin@corp.nstu.ru

Попова Юлия Александровна, лаборант инжинирингового центра «Информационная безопасность» Новосибирского государственного технического университета. E-mail: yu.popova.2019@stud.nstu.ru

DOI: 10.17212/2782-2230-2023-4-9-23

Methodology for organizing the process of monitoring of distributed information systems*

A.V. Ivanov[1], I.A. Ognev[2], I.V. Nikroshkin[2], J.A. Popova[4]

[1] *Institute of Computational Mathematics and Mathematical Geophysics of Siberian Branch of Russian Academy of Sciences, 6 Akademika Lavrentiev Avenue, Novosibirsk, 630090, Russian Federation, senior researcher at the laboratory of Artificial Intelligence and Information Technologies. E-mail: andrej.ivanov@corp.nstu.ru*
[2] *Institute of Computational Mathematics and Mathematical Geophysics of Siberian Branch of Russian Academy of Sciences, 6 Akademika Lavrentiev Avenue, Novosibirsk, 630090, Russian Federation, engineer at the laboratory of Artificial Intelligence and Information Technologies. E-mail: i.ognev.2016@corp.nstu.ru*
[3] *Institute of Computational Mathematics and Mathematical Geophysics of Siberian Branch of Russian Academy of Sciences, 6 Akademika Lavrentiev Avenue, Novosibirsk, 630090, Russian Federation, engineer at the laboratory of Artificial Intelligence and Information Technologies. E-mail: i.nikroshkin@corp.nstu.ru*
[4] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant at the engineering center "Information Security". E-mail: yu.popova.2019@stud.nstu.ru*

This article is devoted to the methodology of organizing the process of monitoring of distributed information systems. The article considers the general concept of building the process of information security monitoring. Special attention is paid to such disadvantages of distributed systems as problems of system administration, problems of limited scalability of distributed systems and problems of software portability. It was concluded that at present there is no unified approach to eliminate these disadvantages when building a monitoring process. The model of decentralized distributed system for which the methodology of monitoring process organization is developed is given. Three approaches to the organization of monitoring process of distributed information systems are described, namely the organization of monitoring of network activity of information system, the organization of monitoring of host activity of information system and mixed approach. The mixed approach based on monitoring of network and host activity is used in the methodology. The process of prioritization of sources of information security events is considered, which includes the assessment of IS risks, identification of actual IS threats and identification of critical assets of the organization. As a result, a methodology for organizing the process of monitoring distributed information systems is proposed, which consists of four stages: risk calculation, identification of actual threats, prioritization of information security event sources and connection of selected sources to the information security event monitoring system.

Keywords: information security, cybersecurity, monitoring, distributed information systems, monitoring center, SOC, information security events, information security incidents

* *Received 10 November 2023.*

REFERENCE

1. Po dannym Sophos, vremya prebyvaniya zloumyshlennikov v seti uvelichilos' na 36 % [According to Sophos, the time attackers spend on the network has increased by 36 %]. *SecurityLab.ru*, 2022, 9 June. (In Russian). Available at: https://www.securitylab.ru/finance_news/532207 (accessed 01.11.2023).

2. Strelnikov R.V. SOC. Neeffektivnost' vnedreniya [SOC. Inefficiency of implementation]. *Vestnik Baltiiskogo federal'nogo universiteta im. I. Kanta. Seriya: Fiziko-matematicheskie i tekhnicheskie nauki = Vestnik of Immanuel Kant Baltic Federal University. Series: Physical-mathematical and technical sciences*, 2019, no. 4, pp. 81–85.

3. Muniz J., McIntyre G., AlFardan N. *Security operations center: building, operating, and maintaining your SOC*. Cisco Press, 2015. Available at: http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052076 (accessed 01.12.2023).

4. Kazantsev A., Krasov A., Katasonov A., Gelfand A. [Formation and control of Security Operations Center (SOC) for efficient using in practice]. *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii*. VIII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya [8th International Conference on Advanced Infotelecommunications ICAIT 2019]. St. Petersburg, 2019, pp. 590–595. (In Russian).

5. Mughal A.A. Building and securing the modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, 2022, vol. 5 (1), pp. 1–15.

6. Alahmadi B.A., Axon L., Martinovic I. 99 % false positives: a qualitative study of SOC analysts' perspectives on security alarms. *31st USENIX Security Symposium*. Boston, USENIX Association, 2022, pp. 2783–2800.

7. Shahjee D., Ware N. Integrated network and Security Operation Center: a systematic analysis. *IEEE Access*, 2022, vol. 10, pp. 27881–27898.

8. Tanenbaum A.S., Steen M. van. *Raspredelennye sistemy. Printsipy i paradigm* [Distributed systems: principles and paradigms]. St. Petersburg, Piter Publ., 2003. 876 p. (In Russian).

9. Tsvetkov V.Ya., Alpatov A.N. Problemy raspredelennykh sistem [Problems of distributed systems]. *Perspektivy nauki i obrazovaniya = Perspectives of Science and Education*, 2014, no. 6 (12), pp. 31–36.

10. Ob ustanovke konveyyerov obrabotki sobytiy [About installing event processing pipelines]. *Positive Technologies. Dokumentatsiya po produktam* [Positive Technologies. Product documentation]. Available at: https://help.ptsecurity.com/projects/siem/latest/ru-RU/help/3690716683 (accessed 01.12.2023).

11. KOMRAD Enterprise SIEM. *Eshelon. Kompleksnaya bezopasnost'* [Echelon. Information security]. Available at: https://npo-echelon.ru/production/65/11793 (accessed 01.12.2023).

12. RuSIEM. (In Russian). Available at: https://rusiem.com/ru/products/rusiem (accessed 01.12.2023).

13. Durnov R.V. Model' raspredelennoi vychislitel'noi seti [Distributed computing network model]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2022, no. 9, pp. 151–153.

14. Dudnikova A.I. Development of a network traffic monitoring system based on Flow protocols. *Molodezh'. Obshchestvo. Sovremennaya nauka, tekhnika i innovatsii = Youth. Society. Modern science, technologies & innovations*, 2021, no. 20, pp. 193–195.

15. Kim S., Park K.-J., Lu C. A survey on network security for cyber–physical systems: from threats to resilient design. *IEEE Communications Surveys & Tutorials*, 2022, vol. 24 (3), pp. 1534–1573. DOI: 10.1109/COMST.2022.3187531.

16. Martins I., Resende J.S., Sousa P.R., Silva S., Antunes L., Gama J. Host-based IDS: a review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems*, 2022, vol. 133, pp. 95–113.

17. Formby D., Beyah R. Temporal execution behavior for host anomaly detection in programmable logic controllers. *IEEE Transactions in Information Forensics and Security*, 2020, vol. 15, pp. 1455–1469.

18. Skendžić A., Kovačić B., Balon B. Management and monitoring security events in a business organization – SIEM system. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, 2022, pp. 1203–1208.

19. Thursday Ehis A.-m. Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture. *Archives of Advanced Engineering Science*, 2023, pp. 1–10. DOI: 10.47852/bonviewAAES32021068.

20. Biryukov S.A., Dyakov S.A. Primenenie metodiki upravleniya riskami v malykh i srednikh stroitel'nykh organizatsiyakh [Application of risk management techniques in small and medium-sized construction companies]. *Vestnik Akademii znanii = Bulletin of the Academy of Knowledge*, 2021, no. 42 (1), pp. 36–45.

21. Xiong W., Legrand E., Åberg O., Lagerström R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 2022, vol. 21 (1), pp. 157–177. DOI: 10.1007/s10270-021-00898-7.

22. FSTEC of Russia. *The methodological document "Methodology for assessing information security threats"* (approved by FSTEC of Russia 05.02.2021, as amended 06.12.2022). (In Russian).

Для цитирования:

Методика организации процесса мониторинга распределенных информационных систем / А.В. Иванов, И.А. Огнев, И.В. Никрошкин, Ю.А. Попова // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 9–23. – DOI: 10.17212/2782-2230-2023-4-9-23.

For citation:

Ivanov A.V., Ognev I.A., Nikroshkin I.V., Popova Yu.A. Metodika organizatsii protsessa monitoringa raspredelennykh informatsionnykh sistem [Methodology for organizing the process of monitoring of distributed information systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 9–23. DOI: 10.17212/2782-2230-2023-4-9-23.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111). – 24–34

УПРАВЛЕНИЕ В СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

УДК 519.24 DOI: 10.17212/2782-2230-2023-4-24-34

РАЗРАБОТКА БАЗЫ ДАННЫХ ДЛЯ ОБРАБОТКИ ИНФОРМАЦИИ О ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ УЧАЩИХСЯ СРЕДНЕЙ ШКОЛЫ*

Г.В. ТРОШИНА[1], В.И. ЛАРИОНОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры вычислительной техники. E-mail: troshina@corp.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники E-mail: vlarionov932@gmail.com.ru*

Базовые информационные системы для сбора общей статистики об учениках и их оценках, о домашних заданиях уже давно широко используются в рамках школьной системы. Но такие системы часто не учитывают потребности учителей и завучей в обработке информации о других достижениях учащихся средней школы, например, об участии в олимпиадах местного и регионального уровня, о спортивных, социальных и других достижениях учеников. Знание этой информации может быть необходимо как для формирования портфолио, так и для участия в различных конкурсах и мероприятиях, проводимых в школе. В таком случае возникает необходимость в создании узконаправленного программного обеспечения, которое позволяет анализировать и оценивать внеурочную деятельность учащихся средней школы. В статье описывается база данных для обработки информации о различных достижениях учащихся среднего школьного образования. Определены связи между таблицами, входящими в состав базы данных. Разработанная база данных позволяет автоматизировать процессы добавления, редактирования и поиска информации о внеурочной деятельности учеников. Реализованы такие возможности, как, например, автоматическая оценка достижений учащихся школьного образования, получение списка учеников школы с градацией по количеству баллов, предоставление статистики по достижениям отдельных учащихся. После установки и первоначальной настройки база данных не требует дополнительного обслуживания. Созданы учетные записи пользователей для разграничения прав доступа различных групп пользователей. Такой подход обеспечивает детализацию уровней безопасности, то есть позволяет указать, что конкретно разрешено пользователю.

Ключевые слова: база данных, внеурочная деятельность, оценка достижений, права доступа, пользователь базы данных, редактирование записей, таблица, статистика достижений

* Статья получена 07 ноября 2023 г.

ВВЕДЕНИЕ

Программное обеспечение в настоящее время является существенной составляющей каждой технологически сложной системы в любой отрасли, будь то связь, энергетика или образование. Да и сами компьютерные технологии вносят значительные изменения в принципы построения таких систем. Всё это требует знаний в области компьютерной архитектуры, архитектуры программного обеспечения и ИТ-стандартов [1–11]. В работе [11] рассматриваются вопросы подготовки отраслевых специалистов с учетом широкого применения компьютерных систем. Функция предоставления управленческой информации с помощью разнообразных систем отчетности становится важной составляющей различных информационных систем.

1. РАЗРАБОТКА СТРУКТУРЫ БАЗЫ ДАННЫХ

В школах, гимназиях и лицеях широко используются информационные системы для сбора статистики об учениках, их оценках, о домашних заданиях учащихся. Но такие системы не учитывают необходимость обработки информации о других достижениях учащихся средней школы (гимназии, лицея), например, об участии в олимпиадах местного и регионального уровня, о спортивных, социальных и других достижениях учеников. В таком случае возникает необходимость в создании специализированного программного обеспечения, которое бы предоставляло возможность анализировать и оценивать внеурочную деятельность учащихся школы (гимназии, лицея).

В качестве среды разработки информационной системы используется инструмент с открытым исходным кодом phpMyAdmin. Ниже перечислены основные достоинства использования этого инструмента:

- Кросс-платформенность;
- нетребовательность
- простота установки;
- простой в использовании графический интерфейс;
- возможность запуска непосредственно на сервере;
- подробная и обширная документация.

Потенциальными пользователями базы данных являются учителя и завучи школы (гимназии, лицея). На рис. 1 приведена структура разработанной базы данных.

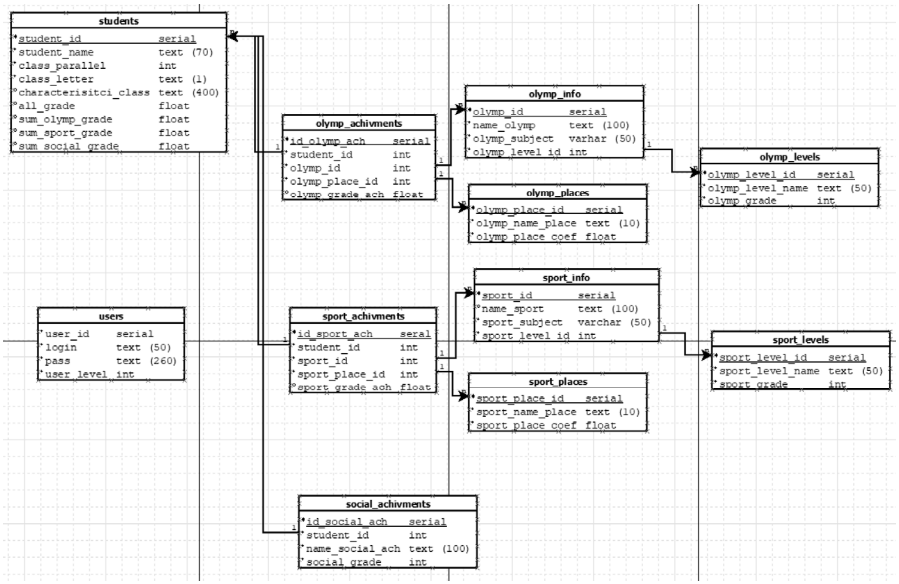

Рис. 1. Структура базы данных

Fig. 1. Database structure

Далее описываются таблицы, входящие в разработанную базу данных. В таблице “students” находится информация об учащихся средней школы (гимназии, лицея):

- student_id – идентификатор ученика;
- student_name – ФИО ученика;
- class_parallel – параллель ученика;
- class_letter – класс ученика;
- characteristic_class – характеристика ученика;
- all_grade – сумма всех оценок ученика за достижения;
- sum_olymp_grade – сумма всех оценок ученика за достижения в олимпиадах;
- sum_sport_grade – сумма всех оценок ученика за спортивные достижения;
- sum_social_grade – сумма всех оценок ученика за социальные достижения.

Таблица-справочник “olymp_levels” содержит информацию об уровнях престижа олимпиад:

- olymp_level_id – идентификатор уровня престижа олимпиады;
- olymp_level_name – имя уровня престижа олимпиады;
- olymp_grade – балльная оценка уровня престижа олимпиады.

Таблица-справочник “olymp_places” включает в себя всю информацию о местах, которые могут занять участники олимпиад:

- olymp_place_id – идентификатор места в олимпиаде;
- olymp_name_place – имя места;
- olymp_place_coef – коэффициент, на который умножается оценка олимпиады за место.

В таблице “olymp_info” находится актуальная информация об олимпиадах, в которых приняли участие ученики школы (гимназии, лицея):

- olymp_id – идентификатор олимпиады;
- name_olymp – имя олимпиады;
- olymp_subject – предмет, к которому относится олимпиада;
- olymp_level_id – идентификатор уровня престижа олимпиады.

Таблица “olymp_achivments” содержит информацию о достижениях учеников школы, полученных в результате участия в олимпиаде:

- id_olymp_ach – идентификатор достижения в олимпиаде одного из учеников;
- student_id – идентификатор ученика;
- olymp_id – идентификатор олимпиады;
- olymp_place_id – идентификатор места в олимпиаде.

Таблица-справочник “sport_levels” содержит информацию об уровнях спортивных соревнований (например, районный, городской или региональный уровень):

- sport_level_id – идентификатор уровня престижа спортивного соревнования;
- sport_level_name – имя уровня престижа спортивного соревнования;
- sport_grade – балльная оценка уровня престижа спортивного соревнования.

Таблица-справочник “sport_places” содержит информацию о местах в спортивном соревновании, которые могут занять участники спортивных мероприятий:

- sport_place_id – идентификатор места в спортивном соревновании;
- sport_name_place – наименование места в спортивном соревновании;
- sport_place_coef – коэффициент, на который умножается оценка спортивного соревнования за место.

В таблице “sport_info” находится информация о спортивных соревнованиях:

- sport_id – идентификатор спортивного соревнования;
- name_sport – имя спортивного соревнования;
- sport_subject – вид спорта, к которому относится спортивное соревнование;
- sport_level_id – идентификатор уровня престижа спортивного соревнования.

Таблица “sport_achivments” содержит информацию о достижениях учеников в спортивных соревнованиях:

- id_sport_ach – идентификатор достижения в спортивном соревновании одного из учеников;
- student_id – идентификатор ученика;
- sport_id – идентификатор спортивного соревнования;
- sport_place_id – идентификатор места в спортивном соревновании.

Таблица – “social_achivments” содержит информацию о социальных достижениях учеников:

- id_social_ach – идентификатор социального достижения одного из учеников;
- student_id – идентификатор ученика;
- name_social_ach – название социального достижения;
- social_grade – балльная оценка социального достижения ученика.

2. УРОВНИ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ

Так как базы данных используются для хранения информации, то это налагает на использование баз данных определенные ограничения. Некоторые записи или таблицы должны быть видны только заранее определенным пользователям. К таблицам, видимым всем, есть разные уровни допуска: не всем разрешено добавлять новые данные или изменять уже существующие данные.

В разработанной базе данных таблица “users” содержит информацию о пользователях информационной системы;

- user_id – идентификатор пользователя;
- login – логин пользователя;
- pass – хэшированный пароль пользователя;
- user_level – уровень доступа пользователя.

Предусмотрено два уровня доступа к данным. Первый уровень – уровень «admin» для завучей, он подразумевает полный доступ к функционалу базы данных. Второй уровень – уровень «user» для учителей, у которого уже огра-

ниченный доступ к таблицам базы данных. При работе с базой данных проверяется, авторизовался ли пользователь. Если пользователь не авторизован, то ему будет предложено авторизоваться. При этом поле ввода пароля имеет функцию «скрытие пароля». Для защиты информации пароль в базе данных хранится в виде хеша. Если пароль успешно введен, то определяется соответствующий уровень доступа пользователя.

3. ТЕХНОЛОГИЯ РАБОТЫ ПОЛЬЗОВАТЕЛЯ

В процессе обработки информации о внеурочной деятельности учащихся предусмотрены следующие варианты работы с базой данных:

- чтение, добавление, редактирование и удаление записей в таблицах базы данных;
- автоматическая оценка всех достижений учеников;
- вывод списка учеников с градацией по количеству баллов;
- предоставление статистики по достижениям учеников;
- создание и вывод портфолио учеников.

У неавторизированного пользователя нет доступа к базе данных, а у пользователя «admin» есть полный доступ ко всему функционалу разработанной базы данных. Пользователь «user» имеет ограниченный доступ к функционалу базы данных. На странице «Статистика» пользователь «user» не имеет ограничений. На них выводится различная информация и статистика, к которой учитель имеет доступ и которая может ему пригодиться (рис. 2).

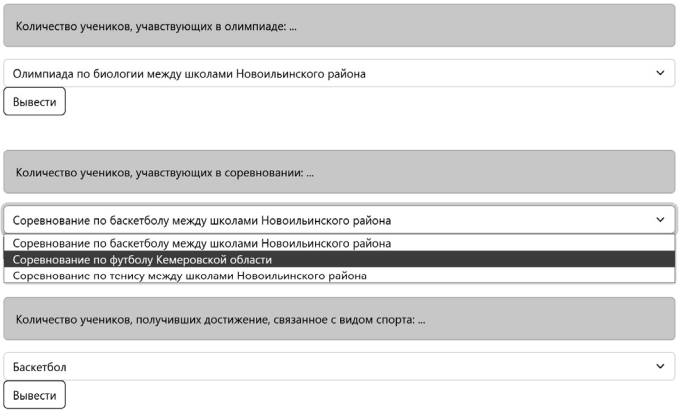

Рис. 2. Страница «Статистика»

Fig. 2. Page «Statistics»

На странице «Редактирование таблиц» можно просмотреть содержание таблиц базы данных, изменить их содержание, а также удалить отдельные записи (рис. 3).

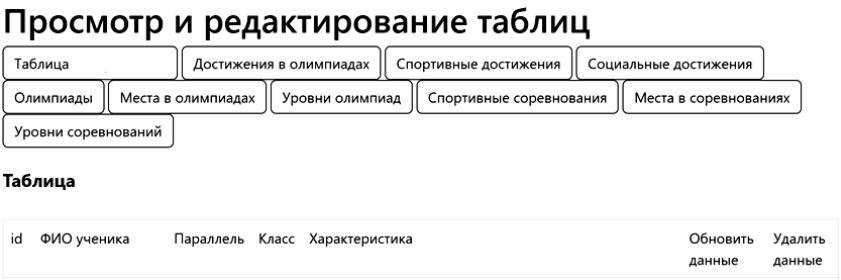

Рис. 3. Страница «Просмотр и редактирование таблиц»

Fig. 3. Page «View and edit tables»

На странице «Добавление новых записей» (рис. 4) у пользователя «user» есть ограничения. Основная задача учителей – вносить достижения учеников в базу данных, поэтому им доступны редактирование имеющихся записей, а также ввод новых записей в таблицы, связанные с этой задачей. Им недоступны таблицы-справочники, а также функция удаления записей.

Рис. 4. Страница «Добавление новых записей»

Fig. 4. Page «Add new records»

Также предусмотрено обеспечение защиты данных от несанкционированного доступа и защита от неправильного ввода информации.

ЗАКЛЮЧЕНИЕ

В настоящей статье описана база данных, предназначенная для обработки информации о внеурочной деятельности учащихся средней школы. Особое внимание уделено вопросам безопасного доступа к данным. Разграничение доступа к данным реализовано через систему паролей. В зависимости от уровня доступа предоставляется соответствующий набор действий, доступных пользователю.

СПИСОК ЛИТЕРАТУРЫ

1. *Конноли Т.*, *Бегг К.* Базы данных: проектирование, реализация и сопровождение. – М.: Вильямс, 2003. – 1436 с.

2. *Хомоненко А.Д.*, *Цыганков В.М., Мальцев М.Г.* Базы данных: учебник для высших учебных заведений. – 4-е изд., доп. и перераб. – СПб.: Корона принт, 2004. – 736 с.

3. *Гольцман В.* MySQL 5.0. – СПб.: Питер, 2010. – 370 с.

4. *Марков А.С., Лисовский К.Ю.* Базы данных: введение в теорию и методологию. – М.: Финансы и статистика, 2004. – 511 с.

5. *Артемов Н.И., Низамутдинов О.Б.* Методическое руководство по проектированию информационных систем CASE-средствами. – Пермь: Изд-во ПГТУ, 1999. – 47 с.

6. *Девис М.Е., Филлипс Дж.А.* Изучаем PHP и MySQL. – СПб.: Символ-плюс, 2008. – 260 с.

7. *Дронов В.А.*PHP 5/6, MySQL 5/6 и Dreamweaver CS4:разработка интерактивных Web-сайтов. – СПб.: БХВ-Петербург, 2009. – 322 с.

8. *Дюваль П., Матиас С., Гловер Э.* Непрерывная интеграция: улучшение качества программного обеспечения и снижение риска. – М.: Вильямс, 2008. – 77 с.

9. PhpStorm. Умная IDE для PHP // JetBrains: сайт. – URL: https://www.jetbrains.com/ru-ru/phpstorm/ (дата обращения: 04.12.2023).

10. WRP. 7 лучших инструментов разработки на PHP для веб-разработки в 2022 году. – URL: https://wrp.ru/statii/7-luchshikh-instrumentov-razrabotki-na-php-dlya-veb-razrabotki-v-2022-godu/ (дата обращения: 04.12.2023).

11. *Romanov E.L., Troshina G.V., Yakimenko A.A.* Software engineering for industry specialists // IV International Conference on Information Technologies in

Engineering Education Inforino 2018, Moscow, 23–26 Oct. 2018: proceedings. – IEEE, 2018. – P. 222–225.

Трошина Галина Васильевна, кандидат технических наук, доцент кафедры вычислительной техники Новосибирского государственного технического университета. Направления научных исследований – базы данных, идентификация динамических объектов. Имеет более 90 публикаций. E-mail: troshina@corp.nstu.ru

Ларионов Владислав Игоревич, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. Направления научных исследований – базы данных, информационные технологии. E-mail: vlarionov932@gmail.com.ru

DOI: 10.17212/2782-2230-2023-4-24-34

Database development for the information processing about extracurricular activities of secondary school students*

G.V. Troshina[1], V.I. Larionov[2]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, associate professor of the computer engineering department. E-mail: troshina@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, master's student of the computer engineering department. E-mail: vlarionov932@gmail.com*

Basic information systems for the general statistics collecting about students and their grades, about homework have long been widely used as part of the school system. But such systems often do not take into account the needs of teachers and head teachers in the information processing about other achievements of secondary school students, for example, participation in local and regional olympiads, about sports, social and other achievements of students. Knowledge of this information may be necessary both to form a portfolio and to participate in various competitions and events held at the school. In this case, it becomes necessary to create narrowly focused software that allows you to analyze and evaluate the extracurricular activities of high school students. This article describes databases for the information processing about various achievements of secondary school students. Relationships between tables that are part of the database are defined. The developed database allows you to automate the processes of adding, editing and the information searching about the extracurricular activities of students. Opportunities have been implemented, such as, for example, the achievements automatic estimation of school students, obtaining a list of school students with gradation by the

* *Received 07 November 2023.*

number of points, and the statistics providing about the achievements of individual students. After installation and initial configuration, the database does not require additional maintenance. User accounts have been created to differentiate the access rights of different user groups. This approach provides details of security levels, that is, allows you to indicate what exactly the user is allowed.

Keywords: database, extracurricular activities, achievement estimation, access rights, database user, records editing, table, achievement statistics

REFERENCES

1. Connolly T.M., Begg C.E. *Bazy dannykh: proektirovanie, realizatsiya i soprovozhdenie* [Database systems: a practical approach to design, implementation, and management]. Moscow, Williams Publ., 2003. 1436 p. (In Russian).

2. Khomonenko A.D., Tsygankov V.M., Mal'tsev M.G. *Bazy dannykh* [Databases]. St. Petersburg, Korona print Publ., 2004. 736 p.

3. Gol'tsman V. *MySQL 5.0*. St. Petersburg, Piter Publ., 2010. 370 p. (In Russian).

4. Markov A.S., Lisovskii K.Yu. *Bazy dannykh: vvedenie v teoriyu i metodologiyu* [Databases: introduction to the theory and methodology]. Moscow, Finansy i statistika Publ., 2004. 511 p.

5. Artemov N.I., Nizamutdinov O.B. *Metodicheskoe rukovodstvo po proektirovaniyu informatsionnykh sistem CASE-sredstvami* [Methodical guide to the information systems design by CASE means]. Perm', PGTU Publ., 1999.47 p.

6. Davis M.E., Phillips D.A. *Learning PHP and MySQL*. Beijing, Sebastopol, Calif., O'Reilly, 2006 (Russ. ed.: Devis M.E., Fillips Dzh.A. *Izuchaem PHP i MySQL*. St. Petersburg, Simvol-plyus Publ., 2008. 260 p.).

7. Dronov V.A. *PHP 5/6, MySQL 5/6 i Dreamweaver CS4: razrabotka interaktivnykh Web-saitov* [MySQL 5/6 and Dreamweaver CS4: interactive websites]. St. Petersburg, BHV-Peterburg Publ., 2009. 322 p.

8. Duvall P.M., Matyas S., Glover A. *Continuous integration: improving software quality and reducing risk*. Upper Saddle River, NJ, Addison-Wesley, 2007 (Russ. ed.: Dyuval' P., Matias S., Glover E. *Nepreryvnaya integratsiya: uluchshenie kachestva programmnogo obespecheniya i snizhenier iska*. Moscow, Williams Publ., 2008. 77 p.).

9. PhpStorm. *JetBrains*. Website. (In Russian). Available at: https://www.jetbrains.com/ru-ru/phpstorm/ (accessed 04.12.2023).

10. WRP. *7 luchshikh instrumentov razrabotki na PHP dlya veb-razrabotki v 2022 godu* [7 best PHP development tools for web development in 2022]. Available at: https://wrp.ru/statii/7-luchshikh-instrumentov-razrabotki-na-php-dlya-veb-razrabotki-v-2022-godu/ (accessed 04.12.2023).

11. Romanov E.L., Troshina G.V., Yakimenko A.A. Software engineering for industry specialists // *IV International Conference on Information Technologies in Engineering Education Inforino 2018*, Moscow, 23–26 Oct. 2018: proceedings. IEEE, 2018, pp. 222–225.

Для цитирования:

Трошина Г.В., Ларионов В.И. Разработка базы данных для обработки информации о внеурочной деятельности учащихся средней школы // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 24–34. – DOI: 10.17212/2782-2230-2023-4-24-34.

For citation:

Troshina G.V., Larionov V.I. Razrabotka bazy dannykh dlya obrabotki informatsii o vneurochnoi deyatel'nosti uchashchikhsya srednei shkoly [Database development for the information processing about extracur-ricular activities of secondary school students]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 24–34. DOI: 10.17212/2782-2230-2023-4-24-34.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111). – 35–46

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.422 DOI: 10.17212/2782-2230-2023-4-35-46

АНАЛИЗ ПРОЦЕССА СОЗДАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ*

Д.О. КУЛИКОВСКИЙ[1], Д.Н. ХАЛИНА[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистр кафедры вычислительной техники. E-mail: kulikovskij.2022@stud.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистр кафедры вычислительной техники. E-mail: khalinadaria@gmail.com*

Статья представляет собой анализ ключевых этапов разработки безопасной информационной системы предприятия. Основное внимание уделяется освещению этапов определения целей информационной безопасности, оценке рисков, идентификации уязвимостей, а также процессу принятия обоснованных решений в контексте обеспечения безопасности информационной системы. Приводятся детальные рекомендации по созданию отчетов о выполненном анализе рисков и процессе принятия обоснованных решений на основе полученных результатов. В рамках работы также проведен анализ процессов составления матрицы вероятности наступления угроз, построения модели нарушителя и этапы построения модели угроз, обеспечивая понимание эффективных рекомендаций для оценки и управления рисками информационной безопасности предприятия и прогнозирования угроз. Также приведены определения всех применяемых терминов и примеры матрицы доступа, матрицы вероятности наступления угроз. Указаны составляющие моделей нарушителя и модели угроз. Отмечены наиболее распространенные ошибки процесса создания отчета об анализе рисков и его представления руководству. Представленный анализ служит важным ресурсом для специалистов по информационной безопасности и руководителей предприятий, которые заинтересованы в построении надежной и безопасной информационной системы.

Ключевые слова: информационная система, безопасность, модель угроз, модель злоумышленника, матрица доступа, матрица угроз, отчет анализа рисков, контроль доступа

* Статья получена 12 ноября 2023 г.

ВВЕДЕНИЕ

На данный момент каждая организация, использующая информационные технологии в целях автоматизации, сталкивается с проблемой обеспечения информационной безопасности. Угрозы как внешнего, так и внутреннего характера наносят многомиллионный ущерб предприятию и его бизнес-процессам [1].

Информационная безопасность – это действия, направленные на предотвращение злонамеренных действий мошенника по отношению к информации вне зависимости от формы воздействия или характера данных.

1. ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ СОЗДАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель построения безопасной информационной системы состоит в сохранении конфиденциальности, доступности и целостности информации. Однако стоимость системы не должна превышать стоимость информации или возможный ущерб от нарушений. Для определения мер, необходимых для вышеуказанных характеристик информации, используется анализ рисков.

2. АНАЛИЗ РИСКОВ

Анализ рисков – это совокупность процедур выявления факторов рисков и оценки их значимости, а также методов снижения вероятности последствий. Поскольку для разных типов информации используются разные методы защиты информации, необходимо четко определить модель злоумышленника. Первоначальная информация о модели злоумышленника запрашивается у руководства, которое имеет представление о ситуации на рынке и располагает сведениями о методах воздействия конкурентов. Наиболее часто используется неформальная модель злоумышленника, отражающая его мотивы или цели (кража информации с целью продажи, нарушение работоспособности сервиса с целью причинения убытков и т. п.) и основные способы их достижения (DDos-атака серверов предприятия, получение удаленного доступа к базам данных с персональной информацией). При моделировании используется теория игр, составляется матрица вероятностей наступления угроз [2]. Рассмотрим пример матрицы вероятностей угроз (табл. 1). В столбцах указан вред, наносимый угрозой в соответствии с ее вероятностью. Обозначим через «Поле **» ситуацию с последствиями, характерными для соответствующей вероятности угрозы.

Таблица 1

Table 1

Матрица вероятности наступления угроз

Threat matrix

Вероятность наступления угрозы	Возможные последствия наступления угрозы			
	Разрушение (Р)	Критические повреждения (К)	Тяжелые повреждения (Т)	Легкие повреждения (Л)
Высокая (В)	Поле ВР	Поле ВК	Поле ВТ	Поле ВЛ
Средняя (С)	Поле СР	Поле СК	Поле СТ	Поле СЛ
Низкая (Н)	Поле НР	Поле НК	Поле НТ	Поле НЛ

После определения основных причин нарушений на них оказывается воздействие или корректируется система защиты. Устранение мотивов или причин, повлекших нарушение, уменьшает вероятность возникновения подобных инцидентов [3]. Также для построения модели нарушителя (рис. 1) используется информация о прецедентах от службы безопасности, сведения о способах хранения и обработки информации, об относящихся к интеллектуальной собственности данных, о способах перехвата передач данных, о конкурентных предприятиях и настроениях в коллективе работников. Дополнительно оцениваются оперативные технические возможности воздействия на системы защищаемого объекта. Технические возможности, или оснащенность, – это средства, оборудование или знания, которыми может располагать злоумышленник. Они подразделяются на физический и логический доступ. Под физическим доступом подразумевается доступ к оборудованию, содержащему искомую злоумышленником информацию. В большинстве случаев физический доступ есть только у сотрудников компании. Логический доступ – это удаленный доступ, реализуемый с использованием вычислительных сетей, позволяющий без физического доступа осуществить доступ к защищаемой информации или выполнить операции по ее обработке [4].

Рис. 1. Модель нарушителя

Fig. 1. Fraudster model

Для проверки нарушения доступа или возможной манипуляции доступом составляется матрица доступа. Это позволяет заметить несанкционированный доступ сотрудников. Матрица доступа представляет собой матрицу, в которой субъекту системы соответствует строка, а объекту – столбец. В клетках матрицы стоят пометки о доступе субъекта к соответствующей системе. Обычно выделяют основные типы разрешенного доступа, такие как «доступ на запись», «доступ на чтение» или «доступ на исполнение». Доступ к объекту может меняться в определенные дни или часы в зависимости от других характеристик объекта или характера проводимых или проведенных работ [5]. В качестве примера матрицы доступа приведена матрица доступов компьютерных пользователей в некоторой сети (рис. 2). За «доступ на запись» отвечает символ «w», за «доступ на чтение» – символ «r» и за «доступ на исполнение» – символ «x». В данной матрице под объектами подразумеваются файлы, а под субъектами – пользователи локальной сети.

Далее в целях создания безопасной информационной системы необходимо построить модель угроз [6]. Важно выяснить связи между информационной инфраструктурой предприятия и информационными активами. Если на предприятии существует четкий регламент обслуживания и эксплуатации оборудования, то сбор информации о типах и вероятностях угроз будет значительно упрощен. Модель угроз состоит из модели нарушителя, информации о системе и базы данных угроз и уязвимостей. Под информацией о системе подразумевается ее программное и аппаратное обеспечение, связи между ее компонентами, задачи и защищаемые ресурсы. База данных содержит пере-

чень угроз информационной безопасности и перечень уязвимостей компонентов системы.

субъекты \ объекты	file1	file2	dir1	file3	docA	docB	docC	docD	dir2	file4	pic1
adm	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx
pgm1	---	---	---	r-x	---	---	---	---	rwx	rwx	---
pgm2	rwx	rwx	rwx	r-x	---	---	---	---	rwx	rwx	---
pgm3	rwx	rwx	rwx	---	---	---	---	---	---	---	---
op1	---	---	rwx	r-x	---	---	---	---	---	---	---
op2	---	---	rwx	r-x	---	---	---	---	---	---	---
op3	---	---	rwx	r-x	---	---	---	---	---	---	---
us1	--x	---	r--	---	rwx	rwx	---	r--	---	---	---
us2	---	---	r--	---	r--	r--	---	r--	---	---	---
us3	--x	---	r--	---	r--	r--	rwx	rwx	---	---	rwx

Рис. 2. Матрица доступа

Fig. 2. Access matrix

Построение модели угроз состоит из пяти последовательных шагов [7].

1. Определение источников угроз.
2. Выявление уязвимых объектов системы.
3. Определение перечня угроз для каждого объекта.
4. Выявление способов реализации угроз.
5. Оценка ущерба от угроз и их последствий.

После разработки модели угроз необходимо идентифицировать и оценить уязвимости для соответствующих активов. Этот процесс выполняется в рамках аудита. Необходимо разработать критерии оценивания на основании информации, представленной в модели угроз и модели злоумышленника.

3. ОЦЕНКА РИСКОВ

Поскольку ущерб оценивается на этапе построения модели угроз, необходимо провести оценку вероятностей событий рисков. Как и оценка активов, оценка вероятности рассчитывается при помощи сводной статистики по инцидентам, предпосылки к которым совпадают с текущими угрозами или ме-

тодом прогнозирования на основе взвешивания факторов, которые соответствуют модели угроз. Прогнозирование вероятности угроз проводится на основе характеристик уязвимостей и злоумышленников. Величину риска необходимо определить для каждого набора вида «актив – угроза», но не в каждом случае вероятность и ущерб могут быть выражены в формате денежного показателя или числа. В каждой компании существует политика управления рисками. Однако в то время как одна организация ставит превыше всего снижение рисков репутации, другая старается контролировать наиболее вероятные риски средней значимости. Если конкретные действия по обработке риска не определены, то производимые работы по снижению рисков должны основываться на максимальной эффективности применимых мер.

На основе полученных в ходе работ результатов разрабатывается простой и наглядный отчет об анализе рисков, целью которого является презентация данных о структуре и значимости рисков информационной безопасности. Этот отчет представляется высшему руководству для принятия решений [8]. Для достижения наглядности отчета схожие риски агрегируются и ранжируются по значимости, а их классификация должна выполняться в привычных бизнес-терминах.

Отчет анализа рисков содержит:

– информацию о наиболее уязвимых областях информационной безопасности;

– анализ влияния угроз на общую структуру рисков;

– наиболее приоритетные направления работы отдела безопасности.

4. АЛГОРИТМ ПРИНЯТИЯ РЕШЕНИЯ

На основе отчета руководство отдела безопасности формирует план работ на среднесрочный период и закладывает бюджет с учетом характера мероприятий по снижению рисков [10]. Так как требования и риски постоянно изменяются, систему безопасности следует не создавать с нуля, а каждый раз модифицировать и дополнять новыми системами защиты. Однако такой подход усложнит процесс проектирования и внедрения. Для функционирования некоторых систем потребуется более высокая пропускная способность оборудования, дополнительные вычислительные мощности и новые сотрудники, обеспечивающие мониторинг и обслуживание средств защиты. В рамках настоящей статьи невозможно рассмотреть конкретные механизмы защиты и их функционал, однако следует заметить, что защитить требуется всю информационную систему. Это влечет за собой повышенные требования к пропускной способности и предельной нагрузке оборудования. Наиболее распространен-

ная ошибка при создании отчета анализа рисков – это представление промежуточных итогов руководству. Отчет должен быть полным, однако в процессе его написания стоит фиксировать этапы готовности.

5. ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Процесс, описанный в настоящей работе, может быть применен на различных уровнях организации, в которой обеспечение информационной безопасности представляет существенное значение.

Применение этого процесса особенно критично для корпоративных предприятий, в которых информационные ресурсы представляют критическую ценность. В этом контексте процесс создания безопасной информационной системы обеспечивает защиту от утечки конфиденциальных данных и нежелательного доступа к корпоративным ресурсам.

Банки, инвестиционные фирмы и другие финансовые учреждения обрабатывают огромные объемы чувствительной информации. Применение данного процесса в этой области позволяет обеспечить безопасность финансовых транзакций, защитить персональные данные клиентов и предотвратить мошенничество.

Защита государственной тайны, информационной безопасности и обеспечение работоспособности критически важных систем – основные моменты, когда применение данного процесса обеспечивает надежную защиту.

Защита медицинской информации, включая конфиденциальные данные пациентов, требует особого внимания к информационной безопасности. Применение рассматриваемого процесса в медицинских учреждениях помогает обеспечить конфиденциальность данных и защиту от угроз нарушения безопасности.

В свете растущей ценности информации ИТ-компании и стартапы обращают всё большее внимание на обеспечение безопасности своих скоростных и инновационных продуктов. Применение данного процесса позволяет им обеспечить надежную защиту своих разработок и данных пользователей.

ЗАКЛЮЧЕНИЕ

Создание систем информационной безопасности предприятия – требующий значительных ресурсов и специализированных знаний и навыков процесс, который включает как проектирование и внедрение средств и систем защиты информации, так и их последующее сопровождение с использованием современных средств, таких как Security Operations Centers.

Анализ рисков, инцидентный менеджмент и аудит информационной безопасности взаимосвязаны, поскольку являются входными и выходными данными вышеуказанных процессов. Внедрение процесса управления рисками необходимо осуществлять с учетом управления инцидентами и аудитом информационной безопасности.

Необходимость проведения анализа рисков становится критической, если организация принимает решение пройти сертификацию по международному стандарту ISO/IEC 27001:2013. Аккредитация соответствующими агентствами проходит поэтапно: сначала изучение аудитором документации системы менеджмента, затем детальный аудит внедренных мер и их эффективности, далее инспекционный аудит соответствия требованиям [11]. Последний этап периодически повторяется в сертифицированных компаниях.

Установление режима защиты конфиденциальной информации и личных данных тесно связано с анализом рисков, поскольку все перечисленные процессы используют сходные методы идентификации и оценки активов, а также разработки моделей нарушителя и моделей угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Создание систем информационной безопасности / Компания «Открытые технологии». – URL: https://www.ot.ru/services/creation-of-information-security/ (дата обращения: 04.12.2023).

2. Матрица вероятностей (рисков) и влияния управления проектов. – URL: https://habr.com/ru/articles/680524/ (дата обращения: 04.12.2023).

3. *Теренин А.* Модель типового злоумышленника и охрана информации. – URL: https://wiseeconomist.ru/poleznoe/57236-model-tipovogo-zloumyshlennika-oxrana-informacii (дата обращения: 04.12.2023).

4. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – М.: Стандартинформ, 2017. – 61 с.

5. *Ясенев В.Н.* Конспект лекций по информационной безопасности / Нижегородский государственный университет им. Н.И. Лобачевского. – Н. Новгород, 2017. – 253 с.

6. Пишем модель угроз // Блог компании «Информационный центр». – 2019, 25 июня. – URL: https://www.google.com/amp/s/habr.com/ru/amp/publications/457516/ (дата обращения: 04.12.2023).

7. *Дроботун Е.Б., Цветков О.В.* Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные про-

дукты и системы. – 2016. – № 3. – С. 42–50. – DOI: 10.15827/0236-235X.115.042-050.

8. *Суханов А.* Анализ рисков в управлении информационной безопасностью // Байт. – 2008. – № 11. – С. 25–29.

9. *Емельянников М.* Информационные системы персональных данных // Журнал «Cio». – 2008. – № 10. – С. 17–20.

10 *Селищев В.А., Чечуга О.В., Наседкин М.Н.* Построение системы информационной безопасности предприятия // Известия Тульского государственного университета. Технические науки. – 2009. – № 1-2. – С. 137–144.

11. *Бирюков Д., Токарева Е.* Международный стандарт ISO/IEC 27001:2013. Взгляд в будущее индустрии ИБ // Информационная безопасность. – 2013. – № 2. – С. 52–55. – URL: https://lib.itsec.ru/articles2/pravo/mezhdunarodnyy-standart-iso-iec-270012013.-vzglyad-v-buduschee-industrii-ib (дата обращения: 05.12.2023).

12. *Бирюков А.А.* Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2013. – 474 с.

13. AEGIS. White paper on research and innovation in cybersecurity. – AEGIS Consortium, 2018.

14. *Mani V.* Cybersecurity and fintech at a crossroads // ISACA Journal. – 2019. – Vol. 2. – P. 1–7.

15. *Dupont B.* The cyber-resilience of financial institutions: significance and applicability // Journal of Cybersecurity. – 2019. – Vol. 5 (1). – P. 1–17.

16. Current cyber-defense trends in industrial control systems / J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez // Computer Security. – 2019. – Vol. 87. – P. 101561.

17. Analysis of intrusion detection systems in industrial ecosystems / J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez // 14th International Conference on Security and Cryptography (SECRYPT 2017). – 2017. – Vol. 6. – P. 116–128.

18. How can organizations develop situation awareness for incident response: a case study of management practice / A. Ahmad, S.B. Maynard, K.C. Desouza, J. Kotsias, M.T. Whitty, R.L. Baskerville // Computer Security. – 2021. – Vol. 101. – P. 102122.

19. Solution-aware data flow diagrams for security threat modeling / L. Sion, K. Yskout, D. van Landuyt, W. Joosen // SAC ’18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. – ACM, 2018. – P. 1425–1432. – DOI: 10.1145/3167132.3167285.

20. Risk-based design security analysis / L. Sion, K. Yskout, D. van Landuyt, W. Joosen // SEAD ’18: Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment. – ACM, 2018. – P. 11–18. – DOI: 10.1145/3194707.3194710.

Куликовский Дмитрий Олегович, студент магистратуры Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: kulikovskij.2022@stud.nstu.ru

Халина Дарья Николаевна, студент магистратуры Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: khalinadaria@gmail.com

DOI: 10.17212/2782-2230-2023-4-35-46

Analysis creation process of a secure enterprise information system*

D.O. Kulikovskij[1], D.N. Khalina[2]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, master's student of the Department of Computer Science. E-mail: kulikovskij.2022@stud.nstu.ru*

[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, master's student of the Department of Computer Science. E-mail: khalinadaria@gmail.com*

The article is an analysis of the key stages of the development of a secure enterprise information system. The focus is on highlighting the stages of determining information security objectives, risk assessment, vulnerability identification, as well as the process of making informed decisions in the context of information system security. The article provides detailed recommendations for creating reports on the completed risk analysis and the process of making informed decisions based on the results obtained. As part of the work, the analysis of the processes of compiling a matrix of the probability of the occurrence of threats, building a model of the violator and the stages of building a threat model was also carried out, providing an understanding of effective recommendations for assessing and managing the risks of information security of the enterprise and forecasting threats. The definitions of all the terms used and examples of the access matrix, the threat probability matrix are also given. The components of the intruder models and threat models are indicated. The most common errors in the process of creating a risk analysis report and presenting it to management are noted. The presented analysis serves as an important resource for information security specialists and business managers who are interested in building a reliable and secure information system.

Keywords: information system, security, threat model, fraudster model, access matrix, threat matrix, risk analysis report, access control

* *Received 12 November 2023.*

REFERENCES

1. Open Technologies. *Sozdanie sistem informatsionnoi bezopasnosti* [Creation of information security systems]. Available at: https://www.ot.ru/services/creation-of-information-security/ (accessed 04.12.2023).

2. *Matritsa veroyatnostei (riskov) i vliyaniya upravleniya proektov* [Matrix of probabilities (risks) and impact of project management] Available at: https://habr.com/ru/articles/680524/ (accessed 04.12.2023).

3. Terenin A. *Model' tipovogo zloumyshlennika i okhrana informatsii* [The model of a typical attacker and information security]. Available at: https://wiseeconomist.ru/poleznoe/57236-model-tipovogo-zloumyshlennika-oxrana-informacii (accessed 04.12.2023).

4. GOST R 57580.1–2017. *Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer* [State Standard R 57580.1–2017. Security of financial (banking) operations. Information protection of financial organizations. Basic set of organizational and technical measures]. Moscow, Standartinform Publ., 2017. 61 p.

5. Yasenev V.N. *Konspekt lektsii po informatsionnoi bezopasnosti* [Lecture notes on information security]. National Research Lobachevsky State University of Nizhni Novgorod, 2017. 253 p.

6. Information Center LLC. *Pishem model' ugroz* [Writing a threat model]. Available at: https://www.google.com/amp/s/habr.com/ru/amp/publications/457516/ (accessed 04.12.2023).

7. Drobotun E.B., Tsvetkov O.V. Postroenie modeli ugroz bezopasnosti informatsii v avtomatizirovannoi sisteme upravleniya kriticheski vazhnymi ob"ektami na osnove stsenariev deistvii narushitelya [Modeling information security threats in the automated control system for crucial objects on the basis of attack scenarios]. *Programmnye produkty i sistemy = Software and Systems*, 2016, no. 3, pp. 42–50. DOI: 10.15827/0236-235X.115.042-050.

8. Sukhanov A. Analiz riskov v upravlenii informatsionnoi bezopasnost'yu [Risk analysis in information security management]. *Bait*, 2008, no. 11, pp. 25–29. (In Russian).

9. Emel'yannikov M. Informatsionnye sistemy personal'nykh dannykh [Information systems of personal data]. *Zhurnal «Cio»*, 2008, no. 10, pp. 17–20. (In Russian).

10. Selischev V.A., Chechuga O.V., Nasedkin M.N. Postroenie sistemy informatsionnoi bezopasnosti predpriyatiya [Building of the system information safety of the enterprise]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2009, no. 1-2, pp. 137–144.

11. Biryukov D., Tokareva E. Mezhdunarodnyi standart ISO/IEC 27001:2013. Vzglyad v budushchee industrii IB [International standard ISO/IEC 27001:2013. A look into the future of information security industry]. *Informatsionnaya bezopasnost' = Information Security*, 2013, no. 2, pp. 52–55. (In Russian). Available at: https://lib.itsec.ru/articles2/pravo/mezhdunarodnyy-standart-iso-iec-270012013.-vzglyad-v-buduschee-industrii-ib (accessed 05.12.2023).

12. Biryukov A.A. *Informatsionnaya bezopasnost': zashchita i napadenie* [Information security: protection and attack]. Moscow, DMK Press, 2013. 474 p.

13. AEGIS. *White paper on research and innovation in cybersecurity*. AEGIS Consortium, 2018.

14. Mani V. Cybersecurity and fintech at a crossroads. *ISACA Journal*, 2019, vol. 2, pp. 1–7.

15. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, 2019, vol. 5 (1), pp. 1–17.

16. Rubio J.E., Alcaraz C., Roman R., Lopez J. Current cyber-defense trends in industrial control systems. *Computer Security*, 2019, vol. 87, p. 101561.

17. Rubio J.E., Alcaraz C., Roman R., Lopez J. Analysis of intrusion detection systems in industrial ecosystems. *14th International Conference on Security and Cryptography (SECRYPT 2017)*, 2017, vol. 6, pp. 116–128.

18. Ahmad A., Maynard S.B., Desouza K.C., Kotsias J., Whitty M.T., Baskerville R.L. How can organizations develop situation awareness for incident response: a case study of management practice. *Computer Security*, 2021, vol. 101, p. 102122.

19. Sion L., Yskout K., Landuyt D. van, Joosen W. Solution-aware data flow diagrams for security threat modeling. *SAC '18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. ACM, 2018, pp. 1425–1432. DOI: 10.1145/3167132.3167285.

20. Sion L., Yskout K., Landuyt D. van, Joosen W. Risk-based design security analysis. *SEAD '18: Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment*. ACM, 2018, pp. 11–18. DOI: 10.1145/3194707.3194710.

Для цитирования:

Куликовский Д.О., Халина Д.Н. Анализ процесса создания безопасной информационной системы предприятия // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 35–46. – DOI: 10.17212/2782-2230-2023-4-35-46.

For citation:

Kulikovskij D.O., Khalina D.N. Analiz protsessa sozdaniya bezopasnoi informatsionnoi sistemy predpriyatiya [Analysis creation process of a secure enterprise information system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 35–46. DOI: 10.17212/2782-2230-2023-4-35-46.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111). – 47–63

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.5 DOI: 10.17212/2782-2230-2023-4-47-63

ФОРМИРОВАНИЕ ТИПОВЫХ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ МОБИЛЬНОГО ПРИЛОЖЕНИЯ*

А.В. НОСЕНКО[1], Т.М. ПЕСТУНОВА[2]

[1] *630090, г. Новосибирск, ул. Пирогова, 2, Новосибирский государственный университет, магистрант направления «Информатика и вычислительная техника» ФИТ. E-mail: a.nosenko1@g.nsu.ru*
[2] *630090, г. Новосибирск, ул. Пирогова, 2, Новосибирский государственный университет, кандидат технических наук, доцент, кафедра компьютерных систем ФИТ. E-mail: t.pestunova@g.nsu.ru*

В статье рассмотрена проблема обеспечения защищенности мобильных приложений, разработка которых часто осуществляется без привлечения специалистов по ИТ-безопасности и в отсутствие доступа к специализированной инфраструктуре программной инженерии. Проанализированы возможные причины недостаточной защищенности мобильного программного обеспечения (МО) и применяемые на практике методы безопасной разработки. На основе лучших практик и рекомендаций разработан базовый перечень требований безопасности к функциям нативного мобильного приложения, инфраструктуре и методам его разработки, реализация которых доступна одиночным разработчикам, не имеющим возможности экспертной поддержки процесса разработки мобильного ПО.

Ключевые слова: мобильное приложение, защита информации, информационная безопасность, безопасное программное обеспечение, требования безопасности, жизненный цикл разработки, тестирование защищенности, угрозы безопасности

ВВЕДЕНИЕ

Мобильные приложения прочно вошли в жизнь организаций и индивидуальных пользователей, деятельность которых подвержена множеству информационных угроз. По статистике, мобильными устройствами пользуется 68 %

* Статья получена 09 ноября 2023 г.

населения мира [1, 12]. Мобильные приложения являются одним из наиболее распространенных объектов атак [3, 7, 17, 18]. Кроме прочего, это можно объяснить и тем, что мобильные устройства стали неотъемлемой частью рабочей среды и коммуникаций, а значит, содержат значительное количество критичной для бизнеса информации.

По оценке экспертов, более 80 % мобильных приложений российских разработчиков содержат уязвимости высокого или критичного уровня [2]. Последние исследования показывают, что наиболее распространены уязвимости небезопасного хранения данных [2, 21]. К примеру, приложения хранят конфиденциальную информацию в исходном коде или в открытом виде. Эти уязвимости являются критическими, поскольку позволяют злоумышленникам получить доступ к конфиденциальной информации пользователей и компаний. Также распространены уязвимости, позволяющие реализовать угрозы целостности приложений. Они могут позволить злоумышленнику изменить логику работы приложения путем модификации кода или внедрения в него вредоносных фрагментов. Например, можно перенаправлять пользователей на фишинговые сайты или перехватывать данные, передаваемые между приложением и сервером. Кроме того, актуальны уязвимости, связанные с сетевой безопасностью, такие как отсутствие шифрования или небезопасная конфигурация сетевого взаимодействия.

Многие из распространенных недостатков мобильных приложений, позволяющих реализовывать эффективные атаки на них, входят в список самых распространенных уязвимостей, по версии OWASP, с 2016 года и по настоящее время [6].

1. СЛЕДОВАНИЕ ЛУЧШИМ ПРАКТИКАМ КАК СПОСОБ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

По оценкам исследователей, при разработке мобильных приложений уделяется недостаточно внимания применению методов безопасного программирования [4, 5, 19]. В целом, аналитики сходятся во мнении, что многие разработчики приложений не имеют достаточной подготовки в практике безопасного программирования. Как правило, повышение квалификации в вопросах ИБ происходит за счет обучения на собственном опыте и требует проявления энтузиазма. Подчеркивается, что нет универсального подхода к мотивации разработчика уделять должное внимание

вопросам безопасности. Главными приоритетами в большинстве случаев являются написание чистого и масштабируемого кода, соблюдение принципов проектирования, в то время как безопасность считается скорее необязательным критерием. Более того, существенно усложняет процесс безопасной разработки отсутствие доступных методов обеспечения безопасности, не требующих привлечения специалистов по ИБ. Таким образом, к основным причинам низкой защищенности мобильных приложений, в частности, можно отнести незаинтересованность разработчиков и отсутствие возможности обращения к специалистам ИБ.

Бизнес, заинтересованный в обеспечении защищенности своих продуктов, выделяет средства на безопасность. По последним отчетам, такие затраты составляют в среднем 30 % от ИТ-бюджета [11]. Обратимся к опыту организаций [8, 22]. Существует множество методов, позволяющих повысить защищенность приложений, среди них обучение разработчиков, проведение «кодревью» и тестирования на проникновение, использование автоматического статического, динамического и интерактивного анализа приложений, выстраивание процесса своевременного обновления зависимостей, моделирование и оценка угроз и в целом построение жизненного цикла безопасной разработки (Security Development Lifecycle). Для выполнения этих задач необходимо привлечение специалистов ИБ.

У индивидуальных разработчиков, в частности, часто отсутствует возможность обращения к специалистам по информационной безопасности. Кроме того, они находятся в условиях ограниченных ресурсов, что делает недоступными некоторые методы обеспечения безопасности. В ходе создания ПО разработчик обычно опирается на собственные знания о безопасности, поэтому их необходимо постоянно актуализировать. Разумно использовать стандарты безопасной разработки, но они сложны для понимания и реализации. Существуют также рекомендации в форме лучших практик. Они могут относиться к некоторой конкретной технологии или фреймворку, носят рекомендательный характер, а при создании защищенного приложения могут быть взяты за основу для определения базовых требований. Их структура должна учитывать три аспекта: требования к процессу разработки, требования к инфраструктуре и функциональные требования безопасности (рисунок).

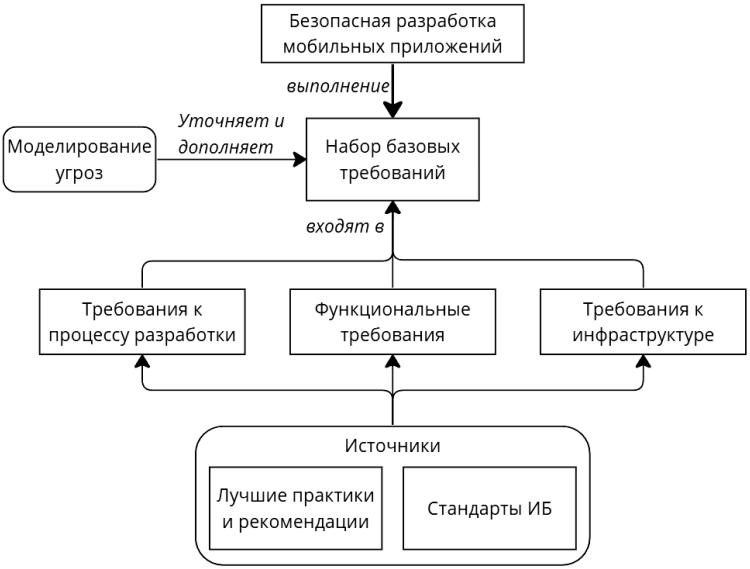

Схема безопасной разработки

Diagram of the system requirements creation process

Для выявления дополнительных требований, направленных на предотвращение актуальных угроз, необходимо проводить периодическое моделирование угроз. Сформированный набор мер может быть использован при разработке методов оценки приложений на предмет соответствия требованиям информационной безопасности.

2. ИСТОЧНИКИ ТРЕБОВАНИЙ

В роли основного источника выступили рекомендации по безопасной разработке от OWASP [13]. Они представляют собой краткое справочное руководство по основным вопросам безопасности приложений, включая практические советы и методы повышения защищенности, а также объяснение рекомендуемых к применению технологий и обоснование требований стандарта MASVS (Mobile Application Security Verification Standard). Стандарт верификации требований к безопасности приложений MASVS является широко используемым многими организациями и специалистами по безопасности во всем мире [9]. Стандарт содержит набор критериев безопасности мобильных

приложений, разделенных по восьми категориям. OWASP рекомендует использовать MASVS как для оценки безопасности продукта, так и в качестве руководства по безопасной разработке. Стандарт поддерживается Google (разработчиком ОС Android), NIST (Национальным институтом стандартов и технологий США) и другими правительственными и образовательными учреждениями. Несомненным преимуществом MASVS является его взаимосвязанность с другими методологиями и стандартами. Во-первых, это CWE – общий перечень недостатков безопасности программного обеспечения. Соответствие между требованиями стандарта и этим перечнем помогает получить представление о потенциальной уязвимости, а также позволяет связывать MASVS с другими стандартами, которые поддерживают CWE, в частности, NIST SP 800-163 [16], Common Criteria for Information Technology Security Evaluation [23] и др. Также стандарт имеет ссылки на MSTG (Mobile Security Testing Guide) – руководство по тестированию защищенности мобильных приложений [15]. Таким образом, все требования стандарта, за исключением требований раздела «Архитектура», имеют соответствующий сценарий проверки выполнимости. Более того, на основе стандарта создан чек-лист MAS (Mobile Application Security), который удобен для применения в процессе разработки и также имеет ссылки на сценарии тестирования. MASVS можно использовать и в качестве инструмента, помогающего обеспечить соответствие мобильных приложений требованиям, изложенным в отраслевых стандартах, поскольку его структура и критерии во многом им соответствуют. В частности, к стандартам, требованиям которых соответствуют рекомендации MASVS, относятся PCI DSS, NIST SP 800-53.

Еще один источник требований – веб-сайт для разработчиков ОС Android [24], на котором предоставлена информация о возможностях платформы, в том числе о функциях безопасности. Документация содержит разделы о безопасности мобильных приложений, включая лучшие практики безопасной разработки с описанием правильного применения функций безопасности Android, рекомендациями по защите передаваемых по сети данных, применению криптографии, хранению конфиденциальной информации и др.

Также источниками требований послужили рекомендации по безопасной разработке от компаний Digital Security [20] и «Стингрей Технолоджиз» [14], специализирующиеся на анализе защищенности мобильных приложений. Digital Security предлагает чек-лист, содержащий требования к использованию нативного API системы, к хранению данных и к архитектуре. Лучшие практики от «Стингрей Технолоджиз» охватывают такие вопросы, как менеджмент ключей и сертификатов, хранение и передача критичной информации, логирование, конфигурация.

3. ОСНОВНЫЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К РАЗРАБОТКЕ И ФУНКЦИЯМ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

На основе перечисленных источников разработан набор базовых требований (табл. 1) к процессу разработки (П) и функциональные требования безопасности (Ф). Требования к инфраструктуре можно рассматривать как требования к инфраструктуре разработчика или к среде функционирования приложения. В приведенных источниках рекомендаций по безопасности для мобильных приложений этот класс требований не рассматривается.

Таблица 1

Table 1

Перечень требований

List of requirements

Ф1. Требования к хранению критичной информации	
Ф1.1. Хранение данных в оперативной памяти	
Требования	
Ф1.1.1	**Необходимо** хранить критичные данные в примитивных типах данных, таких как байтовый или символьный массивы. **Не рекомендуется** использовать неизменяемые и непримитивные типы
Ф1.1.2	Если данные хранятся в непримитивных объектах, то **необходимо** выполнять явный вызов сборщика мусора и корректное удаление ссылок. Ссылки должны быть перезаписаны перед удалением вне метода finalize
Ф1.1.3	Переменные, содержащие конфиденциальную информацию, после использования **необходимо** перезаписать значениями других переменных или случайными значениями. Чтобы обойти оптимизации компилятора, **рекомендуется** сохранить переменные после перезаписи во временный файл, например /dev/null, однако это может негативно сказаться на производительности
Ф1.1.4	**Рекомендуется** обрабатывать критичную информацию минимальным числом компонентов
Ф1.2. Хранение данных на устройстве	
Ф1.2.1	**Рекомендуется** запретить резервное копирование, для этого в манифесте нужно установить значение false параметра allowBackup
Ф1.2.2	Для хранения критичных данных в открытом виде **необходимо** использовать зашифрованные хранилища: Encrypted SQLite Database (SQLCipher), Encrypted Realm Database, EncryptedSharedPreferences, EncryptedFile
Ф1.2.3	Если используется зашифрованное хранилище, то ключ шифрования не должен находиться в коде или храниться в открытом виде. **Рекомендуется** получать ключ из пароля или PIN

Продолжение табл. 1

Continuation of the Tab. 1

Ф1.2.4	Для хранения критичных данных в зашифрованном виде **рекомендуется** использовать хранилища: Shared Preferences, SQLite Database, Realm Database, Internal Storage
Ф1.2.5	Если используется Shared Preferences или Internal Storage, то **необходимо** установить режим MODE_PRIVATE
Ф1.3. Хранение криптографических материалов	
Ф1.3.1	Криптографические материалы **необходимо** хранить в специализированном хранилище (Keychain/Keystore)
Ф1.3.2	Если поддерживаются, то **необходимо** использовать специализированное хранилище с аппаратной поддержкой, иначе **необходимо** использовать программную реализацию
Ф1.3.3	Если используется Keystore API, то **необходимо** использовать AndroidKeystore-реализацию
Ф1.3.4	При использовании AndroidKeystore **необходимо** установить флаг unlockedDeviceRequied в *true* для предотвращения расшифровки ключей приложения при заблокированном устройстве.
Ф1.3.5	При использовании аппаратного хранилища **необходимо** установить флаг setIsStrongBoxBacked в *true* для защиты ключей модулем StrongBox Keymaster
Ф1.3.6	Если используется программная реализация Keystore, то **необходимо** отказаться от явной передачи имени провайдера в KeyStore.getInstance
Ф1.3.7	Если используется программная реализация Keystore, то для разблокировки и проверки ее целостности **необходимо** использовать ключ, который должен быть получен из PIN или пароля пользователя
Ф1.3.8	**Необходимо** использовать биометрическую аутентификацию для управления доступом к элементам Keystore. Биометрическая аутентификация пользователя должна выполняться при каждом использовании ключа
Ф1.3.9	**Необходимо** обеспечить инвалидацию хранимых ключей при регистрации новой биометрической информации
Ф1.4. Валидация данных из общедоступных хранилищ	
Ф1.4.1	**Необходимо** валидировать данные, извлекаемые из общедоступных хранилищ, таких как Shared Preferences. Валидацию **необходимо** производить в момент чтения
Ф1.4.2	**Необходимо** проверять целостность хранимых данных
Ф1.5. Отображение данных в пользовательском интерфейсе	
Ф1.5.1	**Необходимо** отключить кэш-клавиатуры, автозаполнение и проверку правописания для полей ввода критичных данных. Для этого нужно установить флаг *android:inputType textNoSuggestions*
Ф1.5.2	**Необходимо** маскировать поля с критичными данными, чтобы они не были видны через пользовательский интерфейс

Продолжение табл. 1

Continuation of the Tab. 1

Ф1.5.3	**Необходимо** скрывать критичные данные в фоновом режиме
Ф1.5.4	**Необходимо** запретить скриншоты на экранах с критичными данными. Для этого нужно установить флаг *FLAG_SECURE*. Флаг указывает системе, что содержимое экрана не должно попасть в скриншот
Ф2. Требования к аутентификации	
Ф2.1. Общие требования	
Ф2.1.1	Если приложение предоставляет пользователям доступ к удаленным сервисам, **необходимо** проводить аутентификацию на бэкенде
Ф2.1.2	**Необходимо** реализовать безопасный второй фактор аутентификации, такой как OTP на основе времени (Time-based One-time Password Algorithm), push-уведомление или иной, который также необходимо использовать при регистрации и восстановлении аккаунта
Ф2.1.3	Проверку аутентификации **необходимо** проводить до обработки диплинков и push-сообщений
Ф2.1.4	Если используется access-токен, то при включенном входе по PIN-коду или биометрии **необходимо** хранить его только в памяти. Токен не должен храниться на файловой системе устройства
Ф2.1.5	Если используется access-токен, то его **необходимо** подписывать безопасным криптоалгоритмом на бэкенде
Ф2.1.6	Если используются сессии, то идентификатор сессии **необходимо** генерировать случайно на бэкенде с помощью безопасного генератора
Ф2.1.7	Если используются сессии, то **необходимо** удалять на бэкенде существующую сессию при выходе пользователя из системы
Ф2.1.8	Если пользователь аутентифицируется по паролю, то **необходимо** настроить парольную политику. **Рекомендуется** установить минимальную длину пароля в 12 символов и разрешить любые печатные символы Unicode
Ф2.1.9	Если пользователь аутентифицируется по паролю, то **необходимо** предоставить возможность менять пароль. При смене пароля **необходимо** ввести старый и новый пароли. При смене пароля **необходимо** сбрасывать существующие сессии и токены
Ф2.1.10	**Необходимо** реализовать на бэкенде защиту от перебора авторизационных данных
Ф2.1.11	**Необходимо** предоставить пользователю возможность просматривать список устройств и сессий и возможность блокировать определенные устройства, а также инвалидировать определенную сессию
Ф2.2. Требования к аутентификации по PIN-коду	
Ф2.2.1	Необходимо избегать хранения PIN-кода на устройстве или серверной части
Ф2.2.2	Для генерации ключа шифрования из PIN необходимо использовать криптостойкие алгоритмы формирования ключа, такие как Argon2 или PBKDF2

Продолжение табл. 1

Continuation of the Tab. 1

Ф2.2.3	При реализации шифрования **необходимо** соблюдать требования по выбору алгоритма шифрования, длины ключа, криптографических параметров и материалов, описанных в разделе *3.3 Шифрование*
Ф2.3. Требования к биометрической аутентификации	
Ф2.3.1	**Необходимо** основывать биометрическую аутентификацию на разблокировке доступа к записям в Keychain/Keystore. Нельзя основывать ее на определенном событии, таком как вызов api
Ф2.3.2	При изменении настроек биометрии вход в приложение по ним должен блокироваться, для этого **необходимо** проверять наличие изменений в хранилище после входа
Ф3. Требования к криптографии	
Ф3.1. Генераторы случайных чисел	
Ф3.1.1	Генерацию криптографически сильных случайных чисел **необходимо** производить встроенными средствами языка программирования
Ф3.1.2	Для инициализации генератора **необходимо** использовать значение с достаточной энтропией
Ф3.1.3	Для генерации криптографически сильных случайных чисел **необходимо** использовать java.security.SecureRandom. **Рекомендуется** использовать метод getInstanceStrong()
Ф3.1.4	**Необходимо** выбирать стойкий алгоритм генерации. По умолчанию используется стойкий NativePRNGBlocking
Ф3.2. Управление ключами	
Ф3.2.1	**Необходимо** импортировать ключи только из доверенных мест
Ф3.2.2	Генерацию симметричного ключа из пароля **рекомендуется** производить с помощью алгоритма PBKDF2
Ф3.2.3	Для генерации пары публичного и приватного ключа **рекомендуется** использовать KeyPairGenerator с KeyGenParameterSpec
Ф3.2.4	Для генерации симметричного ключа **рекомендуется** использовать KeyGenerator с KeyGenParameterSpec, или криптографически стойкий генератор случайных чисел
Ф3.2.5	**Необходимо** безопасно хранить ключи согласно требованиям раздела по хранению криптографических материалов
Ф3.2.6	При передаче ключей между устройствами или между клиентской и серверной частями приложения **необходимо** обеспечить шифрование
Ф3.3. Шифрование	
Ф3.3.1	Криптографические операции **необходимо** осуществлять встроенными средствами Android SDK
Ф3.3.2	**Необходимо** использовать распространенные алгоритмы с доказанной стойкостью, такие как AES или RSA

Продолжение табл. 1

Continuation of the Tab. 1

Ф3.3.3	**Необходимо** выбирать достаточную длину ключа и алгоритм шифрования. Для выбора длины ключа и алгоритма шифрования **рекомендуется** пользоваться стандартом NIST SP 800-57. Нужно ориентироваться на время хранения данных
Ф3.3.4	В качестве симметричного алгоритма шифрования **рекомендуется** использовать AES с длиной ключа 256 бит и GCM-режимом шифрования
Ф3.3.5	В качестве асимметричного алгоритма шифрования **рекомендуется** использовать RSA с длиной ключа 3072 бит
Ф3.3.6	Для генерации случайных значений **необходимо** использовать криптографически стойкие генераторы случайных чисел
Ф3.3.7	**Необходимо** обеспечить уникальность вектора инициализации
Ф3.3.8	**Необходимо** использовать безопасный режим блочного шифрования. Рекомендуется CBC
Ф3.3.9	**Необходимо** использовать PKCS7 алгоритм дополнения
Ф3.4. Контроль целостности и HMAC	
Ф3.4.1	Генерацию HMAC **необходимо** осуществлять исключительно встроенными средствами языка
Ф3.4.2	**Необходимо** использовать безопасные алгоритмы хеширования: SHA-256, SHA-384, SHA-512, Blake2, SHA-3
Ф4. Требования к передаче данных	
Ф4.1	**Необходимо** использовать SSL Pinning или Certificate Transparency (CT). Для поддержки CT рекомендуется использовать библиотеки *Certificate Transparency for Android* и *Conscrypt – A Java Security Provider*
Ф4.2	В WebView **необходимо** использовать SSL Pinning
Ф4.3	Любую передачу данных **необходимо** проводить по защищенному соединению с использованием TLS
Ф4.4	**Необходимо** использовать TLS v1.2 или v1.3
Ф4.5	Если используются TLS v1.0 или v1.1, то **необходимо** отключить поддержку небезопасных шифронаборов. Для определения рекомендованных шифронаборов рекомендуется обратиться к таблице IANA
Ф5. Требования к ведению журнала	
Ф5.1	**Необходимо** избегать попадания критичной информации в журнал
Ф5.2	При отсутствии необходимости вести журнал в производственной версии приложения, **необходимо** удалить все операторы логирования
Ф6. Требования к использованию WebView	
Ф6.1. Общие требования	
Ф6.1.1	**Необходимо** производить сетевое взаимодействие с серверами только по защищенному каналу
Ф6.1.2	**Необходимо** отключить поддержку Javascript, если она не требуется

Окончание табл. 1

End of the Tab. 1

Ф6.2. Требования к ограничению ресурсов	
Ф6.2.1	**Необходимо** настроить белый список разрешенных ресурсов
Ф6.2.2	**Необходимо** настроить белый список разрешенных протоколов. **Рекомендуется** разрешить только https. **Необходимо** запретить поддержку потенциально опасных URL-схем: file, tel, app-id
Ф6.2.3	**Необходимо** создать контрольные суммы для локальных HTML- и Javascript-файлов, загружаемых в WebView, и проверять их во время запуска
Ф6.2.4	**Рекомендуется** использовать SafeBrowsing API библиотеку SafetyNet с возможностью настройки URL-схем
Ф6.2.5	**Рекомендуется** использовать VirusTotal API
Ф6.2.6	**Необходимо** запретить доступ к content provider. Для этого установить setAllowContentAccess в *false*
Ф6.2.7	**Необходимо** запретить доступ к файловой системе. Для этого установить setAllowFileAccess в *false*
Ф6.2.8	**Необходимо** запретить доступ из Javascript, работающего в контексте file:// схемы URL, к содержимому других ресурсов с file:// схемой URL. Для этого флаг setAllowFileAccessFromFileURLs должен быть установлен в *false*
Ф6.2.9	**Необходимо** запретить доступ из Javascript, работающего в контексте file:// схемы URL, к содержимому других ресурсов с любого origin. Для этого флаг setAllowUniversalAccessFromFileURLs должен быть установлен в *false*
Ф6.3. Требования к загрузке локальных ресурсов	
Ф6.3.1	**Необходимо** минифицировать локальные Javascript файлы
Ф6.3.2	**Необходимо** размещать локальные HTML- и JS-файлы в каталоге приложения
Ф6.3.3	**Необходимо** использовать WebViewAssetLoader для доступа к локальным HTML и JS файлам по http://
Ф6.3.4	**Необходимо** запретить возможность изменения имени файла, пути, а также содержимого файла со стороны пользователя
Ф6.4. Требования к загрузке внешних ресурсов	
Ф6.4.1	**Необходимо** проводить сетевое взаимодействие только по https
Ф6.4.2	**Необходимо** запретить возможность изменения URL пользователем
Ф6.4.3	**Необходимо** очищать кэш, хранилище и загруженные ресурсы WebView перед уничтожением WebView
П1. Требования к производственной версии приложения	
П1.1	**Необходимо** отключить режим отладки в производственной версии
П1.2	**Необходимо** подписывать приложение валидным сертификатом и реализовать проверку подписи
П1.3	**Необходимо** удалить файлы с информацией для внутреннего использования, приватные ключи и другую раскрывающую логику информацию
П1.4	**Необходимо** запрашивать только минимальное количество разрешений для правильной работы приложения

Таким образом, функциональные требования включают требования к хранению критичных данных, требования к аутентификации, требования к криптографии, требования к передаче данных по сети, требования к ведению журнала, требования к использованию WebView, требования к сборке. Они согласуются с документацией Android и лучшими практиками от Digital Security и «Стингрей Технолоджиз» (табл. 2).

Таблица 2

Table 2

Соответствие требований и источников

Matching requirements and sources

Раздел	MASVS	ОС Android для разработчиков	Digital Security	«Стингрей Технолоджиз»
Хранение критичной информации	+	+	+	+
Аутентификация	+	+	+	–
Криптография	+	+	+	+
Передача данных	+	+	+	+
Ведение журнала	+	+	+	–
Использование WebView	+	+	+	+
Производственная версия приложения	+	+	+	–

ЗАКЛЮЧЕНИЕ

В результате исследований определены требования безопасности к разработке мобильных приложений. Они могут быть соотнесены с типовыми угрозами безопасности. В целом, данные требования соответствуют стандарту MASVS на уровне L1, за исключением ряда требований (к архитектуре, дизайну, модели угроз и стойкости к некоторым трудоемким атакам), являющихся сложными для реализации разработчиками, не имеющими возможности экспертной поддержки специалистами по безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Digital 2023: Global Overview Report. – URL: https://datareportal.com/reports/digital-2023-global-overview-report (accessed: 05.12.2023).

2. Оценка защищенности мобильных приложений российских разработчиков. Исследование «Стингрей Технолоджиз». – URL: https://stingray-mobile.ru/wp-content/uploads/2022/12/stingray-annual-report-2022.pdf (дата обращения: 05.12.2023).

3. *Шишкова Т.* Развитие информационных угроз в первом квартале 2022 года. Мобильная статистика. – URL: https://securelist.ru/it-threat-evolution-in-q1-2022-mobile-statistics/105235/ (дата обращения: 05.12.2023).

4. *Weir C., Hermann B., Fahl S.* From needs to actions to secure apps? The effect of requirements and developer practices on app security // Proceedings of the 29th USENIX Security Symposium. – USENIX Association, 2020. – P. 289–305. – URL: https://www.usenix.org/system/files/sec20-weir.pdf (accessed: 05.12.2023).

5. *Weir C., Rashid A., Noble J.* How to improve the security skills of mobile app developers? Comparing and contrasting expert views // Proceedings of the 2016 ACM Workshop on Security Information Workers. – USENIX Association, 2016. – URL: https://eprints.lancs.ac.uk/id/eprint/80016/1/SOUPS2016_SIW_AppDev_CW7June16_submitted.pdf (accessed: 05.12.2023).

6. OWASP. Mobile Top 10 2023: Updates. – URL: https://owasp.org/www-project-mobile-top-10/ (accessed: 05.12.2023).

7. *Townsend K.* Как смартфоны стали одной из главных целей кибератак. – URL: https://blog.avast.com/ru/smartphones-and-increasing-mobile-threats-avast (дата обращения: 05.12.2023).

8. *Михайлова А.* Мобильные угрозы и методы борьбы с ними. – URL: https://www.securitylab.ru/analytics/501302.php (дата обращения: 05.12.2023).

9. OWASP. Mobile Application Security. – URL: https://mas.owasp.org/MASVS/ (accessed: 05.12.2023).

10. Mobile Security Primer. – URL: https://books.nowsecure.com/secure-mobile-development/en/primer/mobile-security.html (accessed: 05.12.2023).

11. Калькулятор бюджета на информационную безопасность «Лаборатории Касперского». – URL: https://calculator.kaspersky.com/ru (accessed: 05.12.2023).

12. State of Mobile 2023. – URL: https://www.data.ai/en/go/state-of-mobile-2023/ (accessed: 05.12.2023).

13. OWASP. MASVS Cheat Sheet. – URL: https://cheatsheetseries.owasp.org/IndexMASVS.html (accessed: 05.12.2023).

14. Рекомендации по безопасной разработке приложений. – URL: https://saas.stingray-mobile.ru/knowledgebase/2022.12/rg/ (дата обращения: 05.12.2023).

15. OWASP Mobile Application Security Testing Guide (MASTG). – URL: https://mas.owasp.org/MASTG/ (accessed: 05.12.2023).

16. Vetting the security of mobile applications: NIST SP 800-163 Rev. 1 / M. Ogata, J. Franklin, J. Voas, V. Sritapan, S. Quirolgico. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf (accessed: 05.12.2023).

17. Security risks. – URL: https://developer.android.com/topic/security/risks (accessed: 05.12.2023).

18. 2022 Mobile Security Index Report. – URL: https://www.verizon.com/business/resources/reports/mobile-security-index/ (accessed: 05.12.2023).

19. Mobile application security: a systematic literature mapping / F.G. Rocha, I.M.L. do Nascimento, O.S.F. Campos, R. Santos, G.R. Colaborador // 16th CONTECSI-International Conference on Information Systems and Technology Management. – São Paulo, 2019. – DOI: 10.5748/16CONTECSI/SEC-6100.

20. Digital Security. Чек-лист по безопасной разработке мобильных приложений. – URL: https://dsec.ru/useful-materials/chek-list-po-bezopasnoj-razrabotke/ (дата обращения: 05.12.2023).

21. Кибербезопасность в 2022–2023. Тренды и прогнозы. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/ (дата обращения: 05.12.2023).

22. *Никитин А.* Зачем и как решать проблемы безопасности мобильных приложений? // Информационная безопасность. – 2022. – № 3. – С. 57. – URL: https://www.itsec.ru/articles/zachem-i-kak-reshat-problemy-bezopasnosti-mobilnyh-prilozhenij (дата обращения: 05.12.2023).

23. Common Criteria for Information Technology Security Evaluation. Pt. 1. Introduction and general model: v. 3.1, rev. 5. CCMB-2017-04-001. – Common Criteria, 2017. – 106 p. – URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed: 05.12.2023).

Носенко Алексей Владиславович, магистрант направления «Информатика и вычислительная техника» факультета информационных технологий Новосибирского государственного университета. E-mail: a.nosenko1@g.nsu.ru

Пестунова Тамара Михайловна, кандидат технических наук, доцент кафедры компьютерных систем факультета информационных технологий Новосибирского государственного университета. E-mail: t.pestunova@g.nsu.ru

DOI: 10.17212/2782-2230-2023-4-47-63

Formulating typical security requirements for mobile application development*

A.V. Nosenko[1], T.M. Pestunova[2]

[1] *Novosibirsk State University, 2 Pirogov Street, Novosibirsk, 630090, Russian Federation, master's student in information technologies. E-mail: a.nosenko1@g.nsu.ru*
[2] *Novosibirsk State University, 2 Pirogov Street, Novosibirsk, 630090, Russian Federation, Associate Professor, Department of Computer Systems. E-mail: t.pestunova@g.nsu.ru*

The article examines the problem of ensuring the security of mobile applications, the development of which is often carried out without the involvement of IT security specialists and in the absence of access to a specialized software engineering infrastructure. The possible causes of insufficient security of mobile software (MS) and the methods of safe development used in practice are analyzed. Based on best practices and recommendations, a basic list of security requirements for the functions of a native mobile application, infrastructure and methods of its development has been developed, the implementation of which is available to single developers who do not have the ability to expert support the process of developing mobile software.

Keywords: mobile application, information protection, information security, safe software, security requirements, development life cycle, security testing, security threats

REFERENCE

1. Digital 2023: Global Overview Report. Available at: https://datareportal.com/reports/digital-2023-global-overview-report (accessed 05.12.2023).

2. Assessment of the security of mobile applications of Russian developers. "Stingray Technologies" study. (In Russian). Available at: https://stingray-mobile.ru/wp-content/uploads/2022/12/stingray-annual-report-2022.pdf (accessed 05.12.2023).

3. Shishkova T. *Razvitie informatsionnykh ugroz v pervom kvartale 2022 goda. Mobil'naya statistika* [Development of information threats in the first quarter of 2022. Mobile Statistics]. Available at: https://securelist.ru/it-threat-evolution-in-q1-2022-mobile-statistics/105235/ (accessed 05.12.2023).

4. Weir C., Hermann B., Fahl S. From needs to actions to secure apps? The effect of requirements and developer practices on app security. *Proceedings of the 29th USENIX Security Symposium*. USENIX Association, 2020, pp. 289–305. Available at: https://www.usenix.org/system/files/sec20-weir.pdf (accessed 05.12.2023).

* *Received 09 November 2023.*

5. Weir C., Rashid A., Noble J. How to improve the security skills of mobile app developers? Comparing and contrasting expert views. *Proceedings of the 2016 ACM Workshop on Security Information Workers*. USENIX Association, 2016. Available at: https://eprints.lancs.ac.uk/id/eprint/80016/1/SOUPS2016_SIW_AppDev_CW7June16_submitted.pdf (accessed 05.12.2023).

6. OWASP. Mobile Top 10 2023: Updates. Available at: https://owasp.org/www-project-mobile-top-10/ (accessed 05.12.2023).

7. Townsend K. *Kak smartfony stali odnoi iz glavnykh tselei kiberatak* [How smartphones have become one of the main goals of cyber-attacks]. Available at: https://blog.avast.com/ru/smartphones-and-increasing-mobile-threats-avast (accessed 05.12.2023).

8. Mikhailova A. *Mobil'nye ugrozy i metody bor'by s nimi* [Mobile threats and methods of combating them]. Available at: https://www.securitylab.ru/analytics/501302.php (accessed 05.12.2023).

9. OWASP. Mobile Application Security. Available at: https://mas.owasp.org/MASVS/ (accessed 05.12.2023).

10. Mobile Security Primer - Available at: https://books.nowsecure.com/secure-mobile-development/en/primer/mobile-security.html/ (accessed date: 10.11.2023).

11. Kaspersky IT Security Calculator. Available at: https://calculator.kaspersky.com/ru (accessed 05.12.2023).

12. State of Mobile 2023. Available at: https://www.data.ai/en/go/state-of-mobile-2023/ (accessed 05.12.2023).

13. OWASP. MASVS Cheat Sheet. Available at: https://cheatsheetseries.owasp.org/IndexMASVS.html (accessed 05.12.2023).

14. Rekomendatsii po bezopasnoi razrabotke prilozhenii [Guidelines for Secure Application Development]. Available at: https://saas.stingray-mobile.ru/knowledgebase/2022.12/rg/ (accessed 05.12.2023).

15. OWASP Mobile Application Security Testing Guide (MASTG). Available at: https://mas.owasp.org/MASTG/ (accessed 05.12.2023).

16. Ogata M., Franklin J., Voas J., Sritapan V., Quirolgico S. *Vetting the security of mobile applications.* NIST SP 800-163 Rev. 1. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf (accessed 05.12.2023).

17. Security risks. Available at: https://developer.android.com/topic/security/risks (accessed 05.12.2023).

18. 2022 Mobile Security Index Report. Available at: https://www.verizon.com/business/resources/reports/mobile-security-index/ (accessed 05.12.2023).

19. Rocha F.G., Nascimento I.M.L. do, Campos O.S.F., Santos R., Colaborador G.R. Mobile application security: a systematic literature mapping. *16th CONTECSI-International Conference on Information Systems and Technology Management*, São Paulo, 2019. DOI: 10.5748/16CONTECSI/SEC-6100.

20. Digital Security. *Chek-list po bezopasnoi razrabotke mobil'nykh prilozhenii* [Checklist for the secure development of mobile applications]. Available at: https://dsec.ru/useful-materials/chek-list-po-bezopasnoj-razrabotke/ (accessed 05.12.2023).

21. Kiberbezopasnost' v 2022–2023. Trendy i prognozy [Cybersecurity in 2022–2023. Trends and forecasts]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/ (accessed 05.12.2023).

22. Nikitin A. Zachem i kak reshat' problemy bezopasnosti mobil'nykh prilozhenii? [Why and how to solve security problems of mobile applications?]. *Informatsionnaya bezopasnost' = Information Security*, 2022, no. 3, p. 57. Available at: https://www.itsec.ru/articles/zachem-i-kak-reshat-problemy-bezopasnosti-mobilnyh-prilozhenij (accessed 05.12.2023).

23. Common Criteria for Information Technology Security Evaluation. Pt. 1. Introduction and general model: v. 3.1, rev. 5. CCMB-2017-04-001. Common Criteria, 2017. 106 p. Available at: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed 05.12.2023).

Для цитирования:

Носенко А.В., Пестунова Т.М. Формирование типовых требований безопасности при разработке мобильного приложения // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 47–63. – DOI: 10.17212/2782-2230-2023-4-47-63.

For citation:

Nosenko A.V., Pestunova T.M. Formirovanie tipovykh trebovanii bezopasnosti pri razrabotke mobil'nogo prilozheniya [Formulating typical security requirements for mobile application development]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 47–63. DOI: 10.17212/2782-2230-2023-4-47-63.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111). – 64–81

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2023-4-64-81

ФОРМИРОВАНИЕ МЕТОДИКИ БЕЗОПАСНОГО ПРОГРАММИРОВАНИЯ ДЛЯ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ*

А.Б. АРХИПОВА[1], Р.Е. ЛИСТАРОВ[2]

[1] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*
[2] *630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: kaf_zi@corp.nstu.ru*

В настоящее время киберфизические системы нередко становятся объектами целевых кибератак, заключающихся в том числе в эксплуатации уязвимостей программного обеспечения, функционирующего в таких системах. Уязвимое программное обеспечение может быть использовано для распространения вредоносных программных средств, кражи или разглашения конфиденциальных данных, воздействия на защищаемую информацию с нарушением установленных прав, приводящих к разрушению, уничтожению, искажению или сбою в работе автоматизированных систем, в которых данное программное обеспечение функционирует. Определение методики безопасной разработки веб-приложений является важнейшим этапом в процессе разработки системы комплексной защиты объекта информатизации. В статье предложены технологии по улучшению уровня защищенности, предоставляемого методикой безопасного программирования BSIMM, с помощью которых можно обеспечить должный уровень защиты для каждого веб-приложения в зависимости от чувствительности обрабатываемой информации.

Ключевые слова: информационная безопасность, защита информации, безопасное программное обеспечение, требования безопасности, жизненный цикл разработки, тестирование защищенности, угрозы безопасности

ВВЕДЕНИЕ

В области информационной безопасности одной из наиболее насущных проблем является обеспечение защиты веб-приложений. Взлом веб-приложений может причинить значительный ущерб системам, которые хранят конфиденциальные и критически важные данные. Статистика показывает, что

* Статья получена 07 ноября 2023 г.

в настоящее время более 80 % кибератак осуществляются через API-интерфейсы, что увеличивает риск для компаний и государственных учреждений [1].

Поэтому формирование методики безопасного программирования, которая поможет снизить риски утечки конфиденциальных данных в веб-приложениях и будет способствовать созданию тестирования для обучения персонала данной методике, является актуальной задачей.

1. КЛАССИФИКАЦИЯ ОСНОВНЫХ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

Основные уязвимости веб-приложений классифицируют согласно OWASP Top 10. Open Worldwide Application Security Project (OWASP) – это некоммерческая организация, работающая над повышением безопасности программного обеспечения. OWASP имеет более 250 отделений по всему миру, десятки тысяч участников, проводит отраслевые, образовательные и обучающие конференции [10].

OWASP Top 10 – это стандартный документ для разработчиков и специалистов по безопасности веб-приложений, обновляющийся каждые 3-4 года и представляющий список наиболее опасных уязвимостей для веб-приложений на данный момент.

Рассмотрим основные группы уязвимостей более подробно.

Нарушение контроля доступа

Контроль доступа обеспечивает соблюдение политики безопасности. Нарушения, как правило, приводят к несанкционированному раскрытию, изменению или уничтожению информации, а также выполнению бизнес-функций, выходящих за пределы прав пользователя.

Перечень основных уязвимостей нарушения контроля доступа представлен ниже.

- Нарушение принципа минимальных привилегий или принципа запрета по умолчанию, когда доступ должен быть предоставлен только для определенных возможностей, ролей или пользователей, но доступен для всех.
- Обход контроля доступа путем изменения URL (манипуляции параметрами или принудительного просмотра), внутреннего состояния приложения или HTML-страницы, а также с использованием инструмента атаки для изменения API-запросов.
- Разрешение просмотра или редактирования учетных записей другого человека путем предоставления ее уникального идентификатора (небезопасные прямые ссылки на объекты).

- Доступ к API без наличия контроля доступа для операций POST, PUT и DELETE.
- Повышение привилегий. Действие в качестве пользователя без авторизации или действие в качестве администратора при входе в систему как обычный пользователь.
- Манипулирование метаданными, такое как повторное использование или изменение токена управления доступом JSON Web Token (JWT), а также изменение cookie или скрытого поля с целью повышения привилегий или злоупотребление отменой JWT.
- Неправильная конфигурация CORS (Cross-Origin Resource Sharing) позволяет получить доступ к API из неподтвержденных / ненадежных источников.
- Принудительный просмотр страниц, требующих аутентификации, в качестве неаутентифицированного пользователя, или принудительный доступ к привилегированным страницам в качестве обычного пользователя.

Контроль доступа эффективен только в надежном серверном коде или в API без сервера, где злоумышленник не может изменить проверку контроля доступа или метаданные.

Криптографические сбои

Криптографические сбои часто приводят к утечке конфиденциальных данных или к нарушению целостности системы. Элементами противодействия криптографическим сбоям являются меры в виде определения требований к защите данных в процессе передачи и хранения, использования современных криптографических функций и схем, анализа эффективности конфигурации и настроек системы.

Инъекции

Приложение становится уязвимым для атак данного типа в следующих случаях:

- входные данные, предоставляемые пользователем, не проходят проверку, фильтрацию или очистку со стороны приложения;
- динамические запросы или непараметризованные вызовы без контекстно осознанной экранировки используются напрямую в интерпретаторе;
- поисковые данные используются в параметрах поиска объектно-реляционного отображения (ORM) для извлечения дополнительных конфиденциальных записей;
- поисковые данные непосредственно используются или конкатенируются. SQL-запрос или команда содержат структуру и вредоносные данные в динамических запросах, командах или хранимых процедурах.

Небезопасный дизайн

Небезопасный дизайн – широкая категория уязвимостей, несущих риск безопасности. Он отличается от небезопасной реализации и имеет свои причины. Отсутствие профилирования бизнес-риска является фактором, способствующим небезопасному дизайну. Поэтому интеграция принципов безопасного программирования на всех жизненных циклах этапов разработки является необходимой составляющей бизнес-процессов организации.

Безопасное программное обеспечение требует применения цикла безопасной разработки, некоторой формы безопасного дизайн-паттерна, методологии, библиотеки безопасных компонентов, инструментария и моделирования угроз. Так, например, следует следить за распределением уровней и слоев систем и сетей, потребление ресурсов для каждого пользователя или сервиса должно быть ограничено.

Неправильная конфигурация

Приложение становится уязвимым для атак данного типа в следующих случаях:

- при отсутствии соответствующей защиты в любой части стека приложения или неправильной настройки разрешения в облачных сервисах;
- включении или установке лишних средств и функций (порты, сервисы, страницы, учетные записи или привилегии) в рамках определенной задачи;
- использовании стандартных учетных записей с неизмененными паролями;
- наличии устаревшего или уязвимого программного обеспечения и других.

Уязвимые и устаревшие компоненты

Приложение становится уязвимым для атак данного типа в следующих случаях:

- если не известны версии всех используемых компонентов (клиентских и серверных);
- программное обеспечение уязвимо, не поддерживается или устарело (включая операционную систему, веб-сервер, сервер приложений, систему управления базами данных, приложения, API, среды выполнения и библиотеки);
- не исправляется или своевременно не обновляется базовая платформа, фреймворки и зависимости. Это часто происходит в средах, где обновления происходят ежемесячно или ежеквартально в рамках процедуры управления изменениями, что оставляет организации открытыми для известных уязвимостей в течение дней или месяцев;
- разработчики программного обеспечения не проверяют совместимость обновленных, улучшенных или исправленных библиотек.

Соответственно для устранения уязвимости «Уязвимые и устаревшие компоненты» должен существовать процесс управления обновлениями. Каждая организация должна обеспечить постоянный мониторинг и применение обновлений или изменений конфигурации на протяжении всего срока эксплуатации приложения или портфолио.

Ошибки идентификации и аутентификации

Подтверждение личности пользователя, аутентификация и управление сеансами являются критическими мерами для защиты от аутентификационных атак.

Могут существовать уязвимости аутентификации в следующих случаях:

- если приложение разрешает автоматизированные атаки, такие как наполнение учетных данных (credential stuffing), когда злоумышленник располагает списком действительных имен пользователей и паролей;
- разрешает атаки методом перебора (brute force) или другие автоматизированные атаки;
- разрешает использование паролей по умолчанию, слабых или широко известных, таких как «Password1» или «admin/admin»;
- использует слабые или неэффективные процессы восстановления учетных данных и восстановления забытого пароля, которые не обеспечивают должную безопасность;
- использует хранение паролей в открытом тексте, шифрованных или слабо хешированных данных;
- отсутствует или неэффективна многофакторная аутентификация;
- показывает идентификатор сеанса в URL;
- повторно использует идентификатор сеанса после успешной аутентификации;
- некорректно отменяет действие идентификатора сеанса.

В качестве противодействия данной уязвимости рекомендуется при возможности реализовать многофакторную аутентификацию для предотвращения автоматического наполнения учетных данных, атак методом перебора и повторного использования украденных учетных данных.

Нарушение целостности данных и программного обеспечения

Сбои программного обеспечения и целостности данных связаны с кодом и инфраструктурой, которые не обеспечивают защиту от нарушений целостности. Примером является ситуация, когда приложение полагается на плагины, библиотеки или модули из ненадежных источников, репозиториев и сетей доставки контента. Небезопасный процесс непрерывной поставки может привести к возможности несанкционированного доступа, внедрения вредоносного кода

или компрометации системы. Кроме того, многие приложения сейчас включают функцию автоматического обновления, при которой обновления загружаются без должной проверки целостности и применяются к ранее доверенному приложению. Злоумышленники могут потенциально загружать свои собственные обновления для распространения и выполнения на всех установках. Еще одним примером является ситуация, когда объекты / данные кодируются или сериализуются в структуру, которую злоумышленник может видеть и изменять, что делает такую систему уязвимой для небезопасной десериализации.

Журнал безопасности и сбои мониторинга

Без ведения журналов и мониторинга невозможно обнаружить нарушения. Недостаточный уровень журналирования, обнаружения, мониторинга и активного реагирования проявляется в следующих случаях:

- события, которые могут быть подвержены аудиту, такие как вход в систему, неудачные попытки входа и транзакции высокой ценности, не регистрируются;
- предупреждения и ошибки не создают или создают недостаточно информативные или понятные журнальные сообщения;
- тестирование на проникновение и сканирование с использованием инструментов динамического тестирования безопасности приложений (DAST) не инициируют оповещений и другие.

Подделка запросов со стороны сервера

Уязвимости данного вида возникают, когда веб-приложение получает удаленный ресурс без проверки предоставленного пользователем URL. Это позволяет злоумышленнику принудить приложение отправить сформированный запрос на неожиданный адрес, даже если он защищен брандмауэром, VPN или другим типом списка управления доступом к сети.

Поскольку современные веб-приложения предоставляют конечным пользователям удобные функции, получение URL становится обычной ситуацией. В результате данная уязвимость становится всё более распространенной [3].

2. СУЩЕСТВУЮЩИЕ МЕТОДИКИ БЕЗОПАСНОГО ВЕБ-ПРОГРАММИРОВАНИЯ

2.1. МЕТОДОЛОГИЯ SDL

Методология разработки программного обеспечения Security Development Lifecycle (SDL) является формальным подходом, который учитывает меры безопасности и конфиденциальности на всех этапах разработки. Она помогает

разработчикам создавать программное обеспечение высокой степени защищенности, обеспечивает соблюдение требований безопасности и конфиденциальности, а также позволяет снизить затраты на разработку.

Методология включает следующие стадии разработки безопасности программного обеспечения.

1. Обеспечение обучения. Эффективное обучение должно дополнять и укреплять политики безопасности, практики разработки безопасного программного обеспечения, стандарты и требования к безопасности на основе данных или новых технических возможностей. Важно отметить, что безопасность – это задача каждого участника процесса, но необязательно каждый должен быть экспертом по безопасности или стремиться стать опытным тестером на проникновение. Однако каждый должен понимать перспективы злоумышленника и его цели, чтобы повысить осведомленность о важности безопасности для организации.

2. Определение требований безопасности. Неотъемлемой частью разработки высокозащищенных приложений и систем является учет безопасности и конфиденциальности. Независимо от выбранной методологии разработки требования безопасности должны постоянно обновляться, чтобы отразить изменения в функциональности и смену окружения угроз. Наиболее подходящим временем для определения требований безопасности является начальный этап проектирования и планирования, поскольку это позволяет интегрировать безопасность и минимизировать возможные нарушения. Факторы, влияющие на требования безопасности, включают юридические и отраслевые стандарты, внутренние политики и практики программирования, анализ предыдущих инцидентов и известные угрозы. Для отслеживания этих требований необходимо использовать системы учета задач или анализировать данные, полученные в процессе разработки.

3. Определение метрик и отчетов о соответствии. Важно установить минимально допустимые уровни безопасности и обязать команды разработчиков их соблюдать. Раннее определение этих уровней помогает команде понять риски, связанные с проблемами безопасности, обнаруживать и исправлять дефекты безопасности на этапе разработки и применять соответствующие стандарты на протяжении всего проекта. Определение метрик для исправления ошибок включает четкое разграничение уровней серьезности уязвимостей безопасности.

4. Создание модели угроз. В средах с высоким уровнем риска для безопасности следует применять модель угроз. Анализ угроз может быть проведен на уровне компонентов, приложений или системы в целом. Это практика, которая позволяет командам разработчиков тщательно рассмотреть, задокументировать и, что важно, структурированно обсудить возможные послед-

ствия для безопасности в контексте запланированной операционной среды. Применение структурированного подхода к сценариям угроз помогает команде более эффективно и экономично выявлять уязвимости безопасности, оценивать риски от этих угроз, а затем выбирать соответствующие меры безопасности и предпринимать необходимые шаги для устранения угроз.

5. Установка требований к дизайну. Обычно методология SDL рассматривается как набор мер, направленных на обеспечение уверенности и помогающих инженерам внедрять «безопасные функции», то есть функции, разработанные с учетом безопасности. Для достижения этой цели инженеры обычно полагаются на такие функции безопасности, как криптография, аутентификация, журналирование и другие. Но во многих случаях их выбор или реализация оказываются сложными, из-за чего дизайнерские или реализационные решения могут привести к появлению уязвимостей. Поэтому крайне важно последовательно применять эти функции и иметь понимание о том, какую защиту они обеспечивают.

6. Определение и использование криптографических стандартов. С увеличением популярности мобильных и облачных вычислений важно гарантировать защиту всех данных, включая конфиденциальную информацию, а также управляющие и контрольные данные, от несанкционированного раскрытия или изменения при передаче или хранении. Обычно для этой цели используется шифрование. Неправильный выбор в использовании любого аспекта криптографии может иметь серьезные последствия, поэтому рекомендуется разработать четкие стандарты шифрования, которые учитывают детали каждого элемента реализации шифрования. Важно доверить эту задачу экспертам. Хорошим общим правилом является использование только проверенных отраслевых библиотек шифрования и обеспечение их реализации таким образом, чтобы их можно было легко заменить при необходимости.

7. Управление рисками безопасности, связанными с использованием стороннего ПО. В настоящее время большинство программных проектов в значительной степени зависит от использования сторонних компонентов – как коммерческих, так и с открытым исходным кодом. При выборе таких компонентов важно учитывать, какая уязвимость в них может повлиять на безопасность более обширной системы, в которую они интегрируются. Для снижения этого риска необходимо иметь точный список сторонних компонентов и план реагирования на обнаружение новых уязвимостей. Однако стоит также рассмотреть возможность проведения дополнительной проверки в соответствии с рисковой политикой организации, типом используемого компонента и потенциальным влиянием уязвимости на системы безопасности.

8. Использование проверенного инструментария. Определите и опубликуйте список инструментов, которые прошли проверку и были утверждены

для использования, включая соответствующие проверки безопасности, такие как параметры компилятора или компоновщика и предупреждения. Инженеры должны стремиться использовать самую последнюю версию утвержденных инструментов (например, утвержденные версии компилятора) и пользоваться преимуществами новых функций анализа безопасности и механизмов защиты.

9. Использование статических анализаторов кода. Анализ исходного кода перед компиляцией предоставляет высокомасштабируемый метод проверки безопасности кода и помогает гарантировать соблюдение политик безопасного программирования. Статический анализ исходного кода (SAST) обычно интегрируется в процесс фиксации изменений, чтобы обнаруживать уязвимости при каждой сборке или упаковке программного обеспечения. Однако некоторые инструменты внедряются непосредственно в среду разработки, чтобы обнаруживать определенные недостатки, такие как использование небезопасных или запрещенных функций, и заменять их на более безопасные альтернативы в процессе активной разработки. Нет универсального решения, и команды разработчиков должны определить оптимальную частоту проведения SAST и, возможно, использовать несколько подходов, направленных на достижение баланса между производительностью и надлежащим обеспечением безопасности [20].

10. Использование динамических анализаторов кода. Проверка работоспособности полностью скомпилированного или упакованного программного обеспечения во время его работы позволяет проверить функциональность, которая проявляется только при интеграции и запуске всех компонентов. Для этого обычно используется набор предварительно созданных атак или инструментов, специально разработанных для мониторинга поведения приложения и выявления проблем, связанных с повреждением памяти, с привилегиями пользователей и с другими критическими проблемами безопасности. Как и в случае с SAST, здесь нет универсального решения, и хотя некоторые инструменты, такие как инструменты сканирования веб-приложений, могут быть легче интегрированы в процесс непрерывной интеграции и доставки (CI/CD), а другие методы тестирования DAST (например, фаззинг) требуют особого подхода [20, 21].

11. Использование тестирования на проникновение. Penetration-тестирование – это процесс анализа безопасности программной системы, выполняемый квалифицированными специалистами по информационной безопасности, которые имитируют действия хакера. Главная цель теста на проникновение состоит в выявлении потенциальных уязвимостей, вызванных ошибками в написании кода, неправильными настройками системы или другими слабостями, связанными с развертыванием приложения. В результате такого тести-

рования обычно обнаруживается широкий спектр уязвимостей. Проведение Penetration-тестов часто сопровождается автоматическими и ручными проверками кода, чтобы создать условия для обеспечения более глубокого уровня анализа по сравнению с обычными возможностями разработчиков.

12. Установка стандарта реагирования на инциденты. Подготовка стандарта реагирования на инциденты имеет решающее значение для противодействия новым угрозам, которые могут возникнуть со временем. Он должен быть разработан совместно командой реагирования на инциденты информационной безопасности продукта (PSIRT) вашей организации. В рамках стандарта должно быть определено, к кому следует обращаться в случае чрезвычайной ситуации в области безопасности и как устанавливать протоколы для обслуживания безопасности, включая стандарты для кода, полученного от сторонних поставщиков и других групп внутри организации. Стандарт реагирования на инциденты должен быть протестирован до момента его фактического использования, чтобы убедиться в его эффективности [5].

Методология SDL была подвергнута тестированию, которое продемонстрировало ее высокую эффективность, в результате чего она была внедрена в широкомасштабное использование. Эта концепция принесла значительную пользу, поскольку существенно снизила частоту возникновения уязвимостей. С течением времени и благодаря усилиям идеологов и опытных специалистов методология регулярно обновляется и совершенствуется.

2.2. МЕТОДОЛОГИЯ BSIMM

Позднее, с широким распространением модели SDL и ее популярностью на рынке, стало ясно, что необходимо систематизировать накопленные знания о безопасной разработке. Кроме того, требовалось найти способ оценки и измерения эффективности этой концепции. В это время возникла и развилась BSIMM (Building Security In Maturity Model), которая предлагает более структурированное описание методологии SSDL (Secure Software Development Lifecycle). BSIMM помогает организациям планировать, осуществлять и измерять различные инициативы в области обеспечения безопасности [4].

«В 2008 году стало ясно, что организации выбирают разные пути для защиты своего программного обеспечения. Эксперты, входящие в состав нынешней группы Synopsys Software Integrity Group, приступили к сбору данных об этих различных путях с целью изучения организаций, которые были высокоэффективны в области безопасности программного обеспечения, провели личные интервью со специалистами по безопасности в организациях и опубликовали свои выводы» [6].

Методология разделена на 4 крупных домена.

- Управление (Governance) – набор практик, которые отвечают за организацию, управление и оценку эффективности безопасной разработки программного обеспечения (SSDL).
- База знаний (Intelligence) – практики, связанные со сбором и систематизацией информации об информационной безопасности внутри организации. Они направлены на распространение и усвоение практик разработки безопасного ПО в широком масштабе.
- Точки соприкосновения с жизненным циклом разработки ПО (SSDL Touchpoints) – практики, связанные с анализом и оценкой конкретных артефактов и процессов, входящих в жизненный цикл производства программного обеспечения.
- Развертывание и эксплуатация (Deployment) – набор практик, отвечающих за взаимодействие с отделами сетевой и инфраструктурной безопасности и службами технической поддержки.

Каждый из этих доменов, в свою очередь, подразделяется на 3 практики.

В общей сложности в BSIMM13 описано 125 активностей. В рамках практик и уровней зрелости нет строгих правил относительно количества активностей. Каждая активность имеет уникальный идентификатор и последовательную нумерацию.

Уровень зрелости отражает популярность активности среди участников и ее частоту использования. Уровень активности зависит от ее сложности и важности. В зависимости от версии BSIMM уровень активности также может изменяться. Фреймворк безопасной разработки (Software Security Framework, SSF) представляет собой набор руководящих принципов, на которых основывается структура BSIMM.

3. ФОРМИРОВАНИЕ МЕТОДИКИ БЕЗОПАСНОГО ПРОГРАММИРОВАНИЯ

В качестве основы формирования методики безопасного программирования возможно предложить внесение дополнительных разделов в методику BSIMM 13.

1. Искусственный интеллект

В сценариях защиты от несанкционированного доступа искусственный интеллект (ИИ) может быть более эффективным, чем человек, в обнаружении аномалий в корпоративных информационных системах. Например, система ИИ может быстро определить, что пользователь пытается войти в систему с необычного рабочего места, которое не принадлежит этому пользователю.

В таком случае ответом со стороны информационной безопасности может быть идентификация этого события сотрудником службы ИБ и принятие соответствующих мер для защиты системы.

В случаях потери данных ИИ способен предсказывать отказы оборудования, на котором обрабатывается информация, более быстро и точно, чем человек. Кроме того, нейросети могут предпринимать превентивные меры, такие как миграция данных на резервные мощности, для минимизации рисков потери данных.

Также ИИ может использоваться для обнаружения вредоносного контента. В контексте вредоносного контента понимается вредоносный код, нацеленный на кражу, блокировку санкционированного доступа или уничтожение значимой информации, а также спам или фишинг. В этом случае использование искусственного интеллекта позволяет проводить эвристическое сканирование и блокировать источники вредоносной информации, получаемой через Интернет.

Одним из важных аспектов работы ИИ в информационной безопасности является появление подобия «гонки вооружений» между специалистами ИБ и злоумышленниками. С распространением технологий искусственного интеллекта и машинного обучения злоумышленники также начинают применять нейросети в своих целях. Учитывая эти проблемы, можно сделать вывод, что использование ИИ в области информационной безопасности требует применения передовых разработок в этой сфере.

Таким образом, можно сделать вывод о том, что применение искусственного интеллекта в ИБ позволяет повысить ее эффективность и решить множество проблем, с которыми человеку сложно справиться из-за больших объемов и скорости обработки информации. Однако при разработке систем с использованием ИИ в информационной безопасности необходимо учитывать особенности этой предметной области, включая противодействие со стороны злоумышленников [11].

2. Big Data

В информационной безопасности концепция Big Data означает использование технологии обработки и анализа больших объемов данных с целью обеспечения безопасности. Данная методика предусматривает сбор и анализ данных, полученных из различных источников, включая структурированные и неструктурированные данные, с высокой скоростью обновления. Информация может поступать из информационных систем, бизнес-платформ, систем управления и связи, а также с устройств и датчиков.

Применение больших данных в обеспечении информационной безопасности имеет огромный потенциал, особенно в контексте развития облачных

сервисов и интернета вещей. Рост объемов данных при условии их своевременного и точного анализа позволяет получить более полное представление о процессах информационной безопасности, обнаруживать и анализировать угрозы и принимать эффективные меры по их предотвращению. Использование методов анализа больших данных позволяет повысить осведомленность о наличии или отсутствии угроз, их характере и в результате принимать более эффективные меры по защите информации [8].

При использовании больших данных в стратегии кибербезопасности появляются новые преимущества, но следует помнить, что такая технология также имеет риск быть атакованной. В то время как анализ объемных данных улучшает обнаружение вредоносной активности и предотвращение утечки данных, сама эта новая форма данных может стать источником потенциальных рисков, связанных с утечкой информации. Это может привести к серьезным последствиям для компании, которая использует такую технологию, поэтому ее, в свою очередь, тоже нужно защищать [9].

В результате можно сделать вывод о том, что технологии искусственного интеллекта и больших данных при совместном использовании с BSIMM смогут создать согласованную информационную систему, в которой методология обеспечит надежную защиту технологии больших данных, а Big Data позволит эффективнее выявлять аномалии, вызванные атаками злоумышленников. Таким образом, можно сделать вывод о том, что применение искусственного интеллекта в ИБ позволяет повысить ее эффективность и решить множество проблем, с которыми человеку сложно справиться из-за больших объемов и скорости обработки информации. Однако при разработке систем с использованием ИИ в информационной безопасности необходимо учитывать особенности этой предметной области, включая противодействие со стороны злоумышленников.

ЗАКЛЮЧЕНИЕ

В статье рассмотрены существующие методики безопасного веб-программирования. Предложены технологии по улучшению уровня защищенности, предоставляемого методикой BSIMM. Благодаря методике безопасного программирования можно обеспечить должный уровень защиты для каждого веб-приложения в зависимости от чувствительности обрабатываемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Алекперов З.А.* Обзор популярных уязвимостей веб-приложений и их решений // Аллея науки. – 2019. – № 5 (32), т. 2. – С. 1098–1113. – URL: https://www.elibrary.ru/item.asp?id=38626043 (дата обращения: 06.12.2023).

2. Что такое CI/CD? Разбираемся с непрерывной интеграцией и непрерывной поставкой // Блог компании OTUS. – URL: https://habr.com/ru/companies/otus/articles/515078/ (дата обращения: 06.12.2023).

3. OWASP Top 10:2021. – URL: https://owasp.org/Top10/ (accessed: 06.12.2023).

4. BSIMM: вдумчиво о плюсах и минусах // Блог компании Swordfish Security. – URL: https://habr.com/ru/companies/swordfish_security/articles/680616/ (дата обращения: 06.12.2023).

5. What are the Microsoft SDL practices? – URL: https://www.microsoft.com/en-us/securityengineering/sdl/ (accessed: 06.12.2023).

6. BSIMM 13 foundations report 2022. – URL: https://www.synopsys.com/software-integrity/engage/bsimm-web/bsimm13-foundations#BSIMM13%20Foundations.indd%3A.67583%3A2668 (accessed: 06.12.2023).

7. OWASP. Стандарт верификации требований к безопасности приложений 4.0.3. – URL: https://github.com/OWASP/ASVS/blob/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-ru.pdf (дата обращения: 06.12.2023).

8. Security Vision. Big Data. – URL: https://www.securityvision.ru/info/big_data/ (дата обращения: 06.12.2023).

9. Почему Большие данные (Big Data). – URL: https://club.cnews.ru/blogs/entry/pochemu_bolshie_dannye_big_data_/ (дата обращения: 02.11.2023).

10. OWASP Application Security Verification Standard. – URL: https://owasp.org/www-project-application-security-verification-standard/ (accessed: 06.12.2023).

11. *Антюфеев А.Б.* Применение и проблемы искусственного интеллекта в информационной безопасности при защите бизнеса // Наука и бизнес: пути развития. – 2021. – № 12 (126). – С. 26–28. – URL: https://www.elibrary.ru/item.asp?id=48095280 (дата обращения: 06.12.2023).

12. *Пителинский К.В, Цапин Д.М.* Управление безопасностью информационных потоков методами технологии Big Data // Международный журнал социогуманитарных исследований. – 2021. – № 4 (4). – С. 11–20. – URL: https://www.elibrary.ru/item.asp?id=50198550 (дата обращения: 06.12.2023).

13. Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud / M. Villamizar, O. Garcés, H. Castro, M. Verano, L. Salamanca, R. Casallas, S. Gil // 2015 10th Computing Colombian

Conference (10CCC). – IEEE, 2015. – P. 583–590. – DOI: 10.1109/ ColumbianCC.2015.7333476.

14. *Mikowski M., Powell J.* Single page web applications: JavaScript end-to-end. – Simon and Schuster, 2013. – 432 p.

15. HTTP метод GET / Э.Ф. Насиров, Д.С. Кириллов, М.В. Чернова, Г.Р. Мертинс // Актуальные вопросы современной науки и образования: сборник статей VII Международной научно-практической конференции. – Пенза, 2021. – С. 33–35. – URL: https://naukaip.ru/wp-content/uploads/2021/01/MK-984-1.pdf#page=33 – (дата обращения: 06.12.2023).

16. CI/CD Pipelines evolution and restructuring: a qualitative and quantitative study / F. Zampetti, S. Geremia, G. Bavota, M. Di Penta // 2021 IEEE International Conference on Software Maintenance and Evolution (ICSME). – Luxembourg, 2021. – P. 471–482. DOI: 10.1109/ICSME52107.2021.00048.

17. *Thakur P.* Evaluation and implementation of progressive web application: thesis. – Helsinki Metropolia University of Applied Sciences, 2018. – URL: https://www.theseus.fi/bitstream/handle/10024/142997/PWA%20thesis.pdf (accessed: 06.12.2023).

18. A survey and comparison of relational and non-relational database / N. Jatana, S. Puri, M. Ahuja, I. Kathuria, D. Gosain // International Journal of Engineering Research & Technology. – 2012. – Vol. 1 (6). – P. 1–5. – DOI: 10.1142/9781848168701_0002.

19. *Boonkrong S., Somboonpattanakit C.* Dynamic salt generation and placement for secure password storing // IAENG International Journal of Computer Science. – 2016. – Vol. 43 (1). – P. 27–36. URL: https://www.iaeng.org/IJCS/issues_v43/issue_1/IJCS_43_1_04.pdf (accessed: 06.12.2023).

20. *Li J.* Vulnerabilities mapping based on OWASP-SANS: a survey for static application security testing (SAST) // Annals of Emerging Technologies in Computing (AETiC). – 2020. – Vol. 4 (3). – URL: https://arxiv.org/ftp/arxiv/papers/2004/2004.03216.pdf (accessed: 06.12.2023).

Архипова Анастасия Борисовна, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – математическое моделирование в информационной безопасности, оценка качества социально значимой деятельности. E-mail: arhipova@corp.nstu.ru

Листаров Роман Евгеньевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Направления научных исследований – информационная безопасность, информационные технологии. E-mail: kaf_zi@corp.nstu.ru

DOI: 10.17212/2782-2230-2023-4-64-81

Formation of secure programming methods for development web applications*

A.B. Arkhipova[1], R.E. Listarov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the security department. E-mail: kaf_zi@corp.nstu.ru*

Today, cyberphysical systems often become targets of targeted cyberattacks, including the exploitation of vulnerabilities in software operating in such systems. Vulnerable software can be used to distribute malicious software, steal or disclose confidential data, affect protected information in violation of established rights, leading to destruction, destruction, distortion or malfunction of automated systems in which this software operates. Determining the methodology for the secure development of web applications is the most important stage in the development of a comprehensive protection system for the object of informatization. This article proposes technologies to improve the level of security provided by the BSIMM method of secure programming, with the help of which it is possible to ensure the proper level of protection for each web application, depending on the sensitivity of the information processed.

Keywords: information security, information security, secure software, security requirements, development lifecycle, security testing, security threats

REFERENCES

1. Alekperov Z.A. Obzor populyarnykh uyazvimostei veb-prilozhenii i ikh reshenii [Overview of popular vulnerabilities in web applications and their solutions]. *Alleya nauki = Alley of Science*, 2019, no. 5 (32), vol. 2, pp. 1098–1113. Available at: https://www.elibrary.ru/item.asp?id=38626043 (accessed 06.12.2023).

2. Chto takoe CI/CD? Razbiraemsya s nepreryvnoi integratsiei i nepreryvnoi postavkoi [What is CI/CD? We deal with continuous integration and non-continuous delivery]. Available at: https://habr.com/ru/companies/otus/articles/515078/ (accessed 06.12.2023).

3. OWASP Top 10:2021. Available at: https://owasp.org/Top10/ (accessed 06.12.2023).

4. BSIMM: vdumchivo o plyusakh i minusakh [BSIMM: Thoughtful about pros and cons]. Available at: https://habr.com/ru/companies/swordfish_security/articles/680616/ (accessed 06.12.2023).

* *Received 07 November 2023.*

5. What are the Microsoft SDL practices? Available at: https://www.microsoft.com/en-us/securityengineering/sdl/ (accessed 06.12.2023).

6. BSIMM 13 foundations report 2022. Available at: https://www.synopsys.com/software-integrity/engage/bsimm-web/bsimm13-foundations#BSIMM13%20Foundations.indd%3A.67583%3A2668 (accessed 06.12.2023).

7. OWASP. *Standart verifikatsii trebovanii k bezopasnosti prilozhenii 4.0.3* [Standard for verification of safety requirements of appendices 4.0.3]. Available at: https://github.com/OWASP/ASVS/blob/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-ru.pdf (accessed 06.12.2023).

8. Security Vision. *Big Data*. Available at: https://www.securityvision.ru/info/big_data/ - (accessed 06.12.2023).

9. Why Big Data is the new focus for information security. (In Russian). Available at: https://club.cnews.ru/blogs/entry/pochemu_bolshie_dannye_big_data_/ (accessed 02.11.2023).

10. OWASP Application Security Verification Standard. Available at: https://owasp.org/www-project-application-security-verification-standard/ (accessed 06.12.2023).

11. Antiufeev A.B. Primenenie i problemy iskusstvennogo intellekta v informatsionnoi bezopasnosti pri zashchite biznesa [Application and problems of artificial intelligence in information security in protecting business]. *Nauka i biznes: puti razvitiya = Science and business: development ways*, 2021, no. 12 (126), pp. 26–28. Available at: https://www.elibrary.ru/item.asp?id=48095280 (accessed 06.12.2023).

12. Pitelinskiy K.V, Tsapin D.M. Upravlenie bezopasnost'yu informatsionnykh potokov metodami tekhnologii Big Data [Information flows security management using Big Data technology methods]. *Mezhdunarodnyi zhurnal cotsiogumanitarnykh issledovanii = International Journal of Socio-Humanitarian Research*, 2021, no. 4 (4), pp. 11–20. Available at: https://www.elibrary.ru/item.asp?id=50198550 (accessed 06.12.2023).

13. Villamizar M., Garcés O., Castro H., Verano M., Salamanca L., Casallas R., Gil S. Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud. *2015 10th Computing Colombian Conference (10CCC)*. IEEE, 2015, pp. 583–590. DOI: 10.1109/ColumbianCC.2015.7333476.

14. Mikowski M., Powell J. *Single page web applications: JavaScript end-to-end*. Simon and Schuster, 2013. 432 p.

15. Nasirov E.F., Kirillov D.S., Chernova M.V., Mertins G.R. [HTTP GET method]. *Aktual'nye voprosy sovremennoi nauki i obrazovaniya* [Current issues of modern science and education]. Collection of articles of the VII International Scientific and Practical Conference. Penza, 2021, pp. 33–35. (In Russian). Available at: https://naukaip.ru/wp-content/uploads/2021/01/MK-984-1.pdf#page=33 (accessed 06.12.2023).

16. Zampetti F., Geremia S., Bavota G., Di Penta M. CI/CD Pipelines evolution and restructuring: a qualitative and quantitative study. *2021 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, Luxembourg, 2021, pp. 471–482. DOI: 10.1109/ICSME52107.2021.00048.

17. Thakur P. *Evaluation and implementation of progressive web applic*ation: thesis. Helsinki Metropolia University of Applied Sciences, 2018. Available at: https://www.theseus.fi/bitstream/handle/10024/142997/PWA%20thesis.pdf (accessed 06.12.2023).

18. Jatana N., Puri S., Ahuja M., Kathuria I., Gosain D. A survey and comparison of relational and non-relational database. *International Journal of Engineering Research & Technology*, 2012, vol. 1 (6), pp. 1–5. DOI: 10.1142/9781848168701_0002.

19. Boonkrong S., Somboonpattanakit C. Dynamic salt generation and placement for secure password storing. *IAENG International Journal of Computer Science*, 2016, vol. 43 (1), pp. 27–36. Available at: https://www.iaeng.org/IJCS/issues_v43/issue_1/IJCS_43_1_04.pdf (accessed 06.12.2023).

20. Li J. Vulnerabilities mapping based on OWASP-SANS: a survey for static application security testing (SAST). *Annals of Emerging Technologies in Computing (AETiC)*, 2020, vol. 4 (3). Available at: https://arxiv.org/ftp/arxiv/papers/2004/2004.03216.pdf (accessed 06.12.2023).

Для цитирования:

Архипова А.Б., Листаров Р.Е. Формирование методики безопасного программирования для разработки веб-приложений // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 64–81. – DOI: 10.17212/2782-2230-2023-4-64-81.

For citation:

Arkhipova A.B., Listarov R.E. Formirovanie metodiki bezopasnogo programmirovaniya dlya razrabotki veb-prilozhenii [Formation of secure programming methods for development web ap-plications]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 64–81. DOI: 10.17212/2782-2230-2023-4-64-81.

ПРАВИЛА ДЛЯ АВТОРОВ

УСЛОВИЯ ПРИЕМА СТАТЕЙ

Все статьи и сопровождающие их материалы в журнал подаются через сайт журнала в электронном виде после регистрации всех авторов статьи. Регистрация обязывает каждого автора иметь международный идентификационный номер ORCID. Иные варианты подачи материалов не рассматриваются.

Автор (один из соавторов) в своем личном кабинете выбирает в меню пункт «Подать статью» и вводит все необходимые данные. Своих соавторов при этом он выбирает из списка зарегистрированных пользователей.

Рукопись статьи готовится в соответствии с правилами оформления в редакторе MS Word и прикрепляется в формате *.doc, *.docx.

Сканированные лицензионный договор с подписями авторов и экспертное заключение (цветной режим сканирования, разрешение не менее 600 dpi) необходимо также разместить на сайте журнала в разделе «Подать статью» в формате *.pdf, *.jpg, *.jpeg.

По окончании всех работ обязательно нажать кнопку «Отправить в редакцию».

В редакцию журнала представляются следующие материалы.

1. **Статья**, подготовленная в соответствии с правилами оформления, – печатная версия, 2 экземпляра, подписанных авторами.

2. **Контактная информация** (телефоны рабочий и сотовый, адреса электронной почты, место работы, адрес места работы, должность, ученая степень, ученое звание автора) – печатная версия, 2 экземпляра.

3. **Описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**, подготовленное в соответствии с правилами оформления, – печатная версия, один экземпляр.

4. **Лицензионный договор**, заполненный и подписанный.

5. **Электронная версия статьи, контактной информации, описания статьи для базы данных РИНЦ, сканированный лицензионный договор и экспертное заключение о возможности опубликования (в отдельных файлах на адрес редакции)**.

6. **Согласие на публикацию, обработку и распространение персональных данных авторов статей**.

7. **Экспертное заключение о возможности опубликования**.

Редакцией рассматриваются только те материалы авторов, которые полностью соответствуют вышеобозначенным требованиям. Неполный пакет материалов редакцией не рассматривается.

Подготовленные материалы направляются на почтовый адрес редакции: 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет (НГТУ), корп. 7, ком. 606, в редакцию журнала «Безопасность цифровых технологий».

Все рукописи рецензируются, по результатам рецензирования редколлегия принимает решение о целесообразности опубликования материалов.

ВНИМАНИЕ!

Авторы несут ответственность за оформление, содержание и сам факт публикации статьи. Редакция журнала не несет ответственности за возможный ущерб, вызванный публикацией статьи. При наличии существенных недостатков в оформлении и содержании статьи редакция принимает решение об отклонении статьи без приведения полного перечня ошибок автора.

Ранее опубликованные материалы, а также материалы, представленные для публикации в других журналах, к рассмотрению не принимаются.

ПРАВИЛА ОФОРМЛЕНИЯ

При подготовке документов для отправки в редакцию журнала авторам рекомендуется внимательно прочитать правила и посмотреть примеры оформления статей и всех необходимых сопутствующих документов. Редакция рассматривает статьи, подготовленные как на русском, так и на английском языке. Для опубликования статьи на английском языке необходимо дополнительно предоставить ее русскоязычный вариант, оформленный по правилам журнала (кроме зарубежных авторов).

Перед отправкой рукописи в редакцию авторам необходимо проверить свою статью с помощью системы «Антиплагиат». Принятый редакционной коллегией уровень оригинальности статей должен составлять не менее 85 %.

Чтобы статья была направлена на рецензирование, необходимо подготовить следующее:

1) **статью** в соответствии с правилами оформления;

2) **контактную информацию** в одном файле предоставить по каждому автору: ФИО полностью, ученая степень, ученое звание автора, должность, место работы, адрес места работы, телефон рабочий и мобильный, адрес электронной почты;

3) **описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**;

4) **лицензионный договор** заполнить, бланк лицензионного договора должен быть подписан только авторами (он доступен авторам также в личном кабинете). Если авторов несколько, то необходимо добавить поля на всех авторов и подписать каждому из них;

5) **экспертное заключение** о возможности опубликования, принятое в вашей организации;

6) согласие на публикацию, обработку и распространение персональных данных авторов статей;

7) авторы, не являющиеся сотрудниками НГТУ, предоставляют **сопроводительное письмо** на имя проректора по научной работе НГТУ (ссылка на страницу сайта НГТУ). Письмо нужно подготовить на бланке организации с подписью и печатью руководителя.

ОСНОВНЫЕ РАЗДЕЛЫ ЖУРНАЛА

Автоматизация и управление технологическими процессами и производствами.

Управление в социальных и экономических системах.

Методы и системы защиты информации, информационная безопасность.

RULES FOR AUTHORS

CONDITIONS FOR ACCEPTANCE OF ARTICLES

All articles and their accompanying materials are submitted to the magazine through the magazine's website in electronic form after registration of all the authors of the article. Registration obliges each author to have an international ORCID. No other material supply options are considered.

The author (one of the co-authors) in his personal account selects the item "Submit article" in the menu and enters all the necessary data. At the same time, he selects his co-authors from the list of registered users.

The manuscript of the article is prepared in accordance with the design rules in the MS Word editor and attached in the format * .doc, * .docx.

Scanned license agreement with signatures of authors and expert opinion (color mode scanning, resolution not less than 600 dpi) can also be attached on the website of the magazine in the section "Submit article" in the format * .pdf, * .jpg, * .jpeg.

At the end of all works, be sure to click the "Send to Design" button.

The following materials are provided to the journal editor:

1. **The article**, prepared in accordance with the rules of design, is a private version, 2 copies signed by the authors.
2. **Contact information** (working and cellular phones, e-mail addresses, place of work, address of the place of work, position, scientific degree, academic title of the author) – printed version, 2 copies.
3. **The description of the article** for the database "**Russian Scientific Citation Index (RSCI)**", prepared in accordance with the rules of form-making, is a printed version, one copy.
4. **License agreement** completed and signed.
5. **Electronic version of the article**, contact information, description of the article for the RSCI database, scanned license agreement and expert opinion on the possibility of publication (in separate files to the editorial address).
6. **Consent to the publication, processing and dissemination of the personal data** of the authors of the articles.
7. **Expert opinion** on the possibility of publication.

The editors consider only those materials of the authors that fully meet the above requirements. Incomplete package of materials is not considered by the revision.

The prepared materials are sent to the postal address of the editorial office: 630073, Novosibirsk, Karl Marx Prospekt, 20, Novosibirsk State Technical University (NSTU), building 7, office 606, to the editors of the journal "Digital Technology Security".

All manuscripts were reviewed, and according to the results of the review, the editorial board decided on the appropriateness of publishing the materials.

ATTENTION!

The authors are responsible for the design, content and the fact of publication of the article. The editorial board of the journal is not responsible for possible damage caused by the publication of the article. If there are significant shortcomings in the design and content of the article, the editorial board decides to reject the article without giving a full list of the author's mistakes.

Previously published materials, as well as materials submitted for publication in other journals, are not accepted for consideration.

FORMATTING RULES

When preparing documents for submission to the journal editor, authors are advised to carefully read the rules and see examples of the design of articles and all necessary related documents. The Drafting Committee considered articles prepared in both Russian and English. To publish the article in English, it is necessary to additionally provide its Russian-language version, drawn up according to the rules of the magazine (except for foreign authors).

Before sending the manuscript to the editorial office, authors must check their article using the Antiplagiarism system. The level of originality of articles adopted by the Editorial Board should be at least 85 %.

For the article to be aimed at peer review, you need to prepare the following:

1) **the article** in accordance with the rules of design (volume from 7 to 30 pages);

2) **provide contact information** in one file for each author: full name, degree, academic title of the author, position, place of work, address of the place of work, telephone number of the worker and mobile, e-mail address;

3) **description of the article** for the database "Russian Scientific Citation Index (RSCI)";

4) fill out the **license agreement**, the form of the license agreement must be signed only by the authors (it is also available to the authors in the personal office), if there are several authors, then it is necessary to add fields on all authors and sign each of them;

5) **expert opinion** on the possibility of publication, adopted in your organization;

6) consent to the publication, processing and dissemination of the personal data of the authors of the articles;

7) authors who are not employees of the NSTU provide a **companion letter** addressed to the vice-rector for scientific work of the NSTU (link to the page of the NSTU website). The letter should be prepared on the form of the organization with the signature and seal of the manager.

JOURNAL SECTION

Automation and control of technological processes and productions.
Governance in social and economic systems.
Methods and systems of information protection, information security.