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 Federation

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

16+

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ

ISSN 2782-2230

№ 2 (113) **2024**

СОДЕРЖАНИЕ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

Лицензия № ИД 04303 от 20.03.01. Подписано в печать 21.06.2024. Выход в свет 26.06.2024
Формат 60×84 1/16. Бумага офсетная. Тираж 300 экз. Уч.-изд. л. 5,58
Печ. л. 6,0. Изд. № 87. Заказ № 140. Цена свободная

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

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/

DIGITAL TECHNOLOGY SECURITY

ISSN 2782-2230

№ 2 (113) **2024**

CONTENTS

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

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

License № ID 04303 from 20.03.01. Signed in print June 21, 2024
Date of publication June 26, 2024. Format 60 × 84 1/16
Offset Paper. Circulation is 300 copies. Educational-ed. liter. 5,58. printed pages 6,0
Publishing number 87. Order number 140

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

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 9–24

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-9-24

ОПЫТ ПРОВЕДЕНИЯ КИБЕРУЧЕНИЙ С ИСПОЛЬЗОВАНИЕМ РАЗРАБОТАННОГО СЦЕНАРИЯ*

А.Р. КАСИМОВА[1], Д.А. ВОРОБЬЕВ[2], А.Н. СЕВРУНОВ[3]

[1] *420015, РФ, г. Казань, ул. Карла Маркса, 68, ФГБОУ ВО «КНИТУ», старший преподаватель кафедры «Информационная безопасность». E-mail: kasimovaar@corp.knrtu.ru*
[2] *660037, РФ, г. Красноярск, пр. имени Газеты «Красноярский рабочий», 31, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, ассистент кафедры безопасности информационных технологий. E-mail: h1ppyfox1@gmail.com*
[3] *660037, РФ, г. Красноярск, пр. имени Газеты «Красноярский рабочий», 31, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, ассистент кафедры безопасности информационных технологий. E-mail: alexander.sevrunov@gmail.com*

Угроза кибератак стала серьезной проблемой для организаций, решение которой в том числе лежит и в плоскости моделирования сценариев возможных атак с применением технологий цифровых двойников. Киберполигон, основанный на программном комплексе AMPIRE, используется для изучения воздействия киберугроз. Сценарий действий злоумышленника включает использование различных тактик и уязвимостей, таких как активное сканирование, подготовка ресурсов, уязвимости в общедоступных приложениях, вредоносные ссылки и файлы, а также компрометацию учетных записей пользователей домена. Вектор атаки злоумышленика соотносится с тактиками, техниками и процедурами матрицы Mitre ATT&CK. Уязвимости включают плагин wpDiscuz, Zerologon и последствия использования Wordpress Shell и получения несанкционированного доступа. Проводимые межвузовские киберучения позволили выявить сильные и слабые места, которые необходимо учитывать при проведении следующих мероприятий. Сценарное тестирование с участием вузов показало эффективность комплекса при оценке времени, необходимого для закрытия уязвимостей и устранения последствий. Реализация на киберполигоне разнотипных сценариев с профильным функционалом дает возможность сформировать практические навыки по предотвращению атак на компьютерные сети, а также позволяет анализировать ситуацию, взаимодействовать с другими специалистами-участниками.

* Статья получена 20 марта 2024 г.

Ключевые слова: киберучения, цифровой двойник, mitre att&ck, digital twin, киберполигон, вектор атаки, моделирование, ЛВС

ВВЕДЕНИЕ

Рынок специалистов в области обеспечения информационной безопасности (ИБ) уже сегодня испытывает острую нехватку квалифицированных кадров, и потребность в них будет только увеличиваться.

Наряду с количеством специалистов является наиболее актуальным вопрос качества подготовки специалистов. Увеличение кибератак во втором квартале 2023 года на 38 % по сравнению с аналогичным периодом 2022 года (325 тыс. инцидентов) стимулировало профильное ведомство обновить стандарты подготовки IT-специалистов в сфере кибербезопасности [1].

Укрупненное направление подготовки 10.00.00 – одно из самых востребованных в вузах, для реализации которого требуются специализированные лаборатории, оборудование, сетевые устройства, программное обеспечение и системы моделирования и анализа данных. Стандарты в области подготовки предусматривают возможность замены специально оборудованных помещений их виртуальными аналогами.

Одним из таких универсальных аналогов можется являться киберполигон (цифровой двойник), который представляет собой многофункциональный программно-аппаратный комплекс и предназначен для обучения, подготовки и тренировки специалистов по информационной безопасности.

Использование киберполигона для реализации безопасного сбора, анализа и управления данных внутри системы является перспективным, поскольку не затрагивает реальную инфраструктуру предприятия и «песочницу», контролируемое пространство, которое помимо прочего можно использовать для валидации и верификации данных [2].

При обучении специалистов на киберполигоне важно, чтобы имелась возможность моделирования конкретной сети или IT-инфраструктуры предприятия, возможность пополнения сценариев атак, распределение ролей, сегментируемость, система отчетности, а также возможность командного взаимодействия.

Целью работы стало исследование применения киберполигона в качестве цифрового двойника сети организации для обучения специалистов в области ИБ.

Для достижения поставленной цели были выделены следующие задачи:

- определить уязвимости и последствия от реализации этих уязвимостей для сценария;
- провести межвузовские киберучения на основе разработанного сценария с использованием киберполигона.

1. ОПИСАНИЕ РАБОТЫ КИБЕРПОЛИГОНА

Понятие «цифровой двойник» подробно изучено и описано в [3–11]. Для исследования был создан цифровой двойник информационной системы типового химического предприятия на базе программного комплекса AMPIRE, используемый в лаборатории КНИТУ, – киберполигон [3]. Подсистемы сетевой безопасности, реализуемые на киберполигоне:

- мониторинг и встроенная корреляция (SIEM);
- контроль доступа;
- сигнатурный анализ;
- ретроспективный анализ.

Помимо подсистем сетевой безопасности также реализована система расследования инцидентов [12].

Схема цифрового двойника локально-вычислительной сети представлена на рис 1.

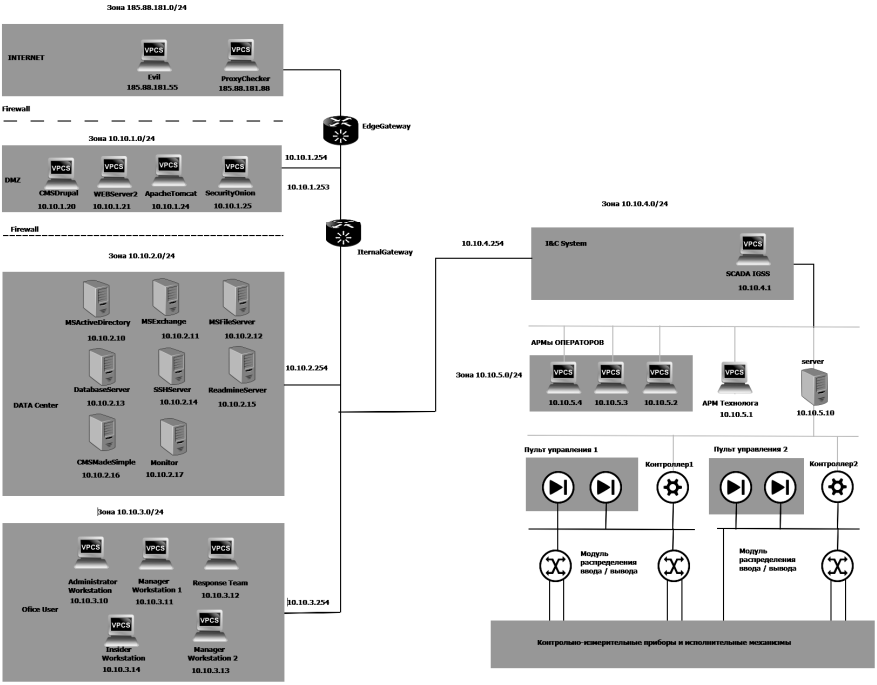


Рис. 1. Схема ЛВС киберполигона

ЛВС представлена пятью зонами:

- сеть Интернет,
- демилитаризованная зона (DMZ),
- центр обработки данных (ЦОД),
- офисные пользователи,
- система ISC.

В качестве средства виртуализации используется специализированное ПО VMWare EXSI. На серверах установлены ОС Linux, для файлового сервера, серверов Active Directory (AD) и Exchange – ОС Windows. На АРМ пользователей установлена ОС Windows и ОС Astra Linux SE 1.6. В качестве базы данных используется MySQL 5.5; IGSS Master используется на АРМ с IP-адресом 10.10.4.1.

2. РАЗРАБОТКА СЦЕНАРИЯ ДЕЙСТВИЯ НАРУШИТЕЛЯ

2.1. ОПИСАНИЕ СЦЕНАРИЯ

Основная цель нарушителя получить доступ к контролеру домена сети – Active Directory (AD). Ядро разработки сценария – матрица MITRE ATT&CK, описывающая тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру. Согласно матрице [13] злоумышленнику будет необходимо использовать следующие тактики и техники:

- тактика – разведка;
- техника – CT1595 «Активное сканирование».

Нарушитель проводит сканирование сети 185.88.181.0/24 и находит сайт с версией Wordpress 5.8.2 с установленным плагином wpDiscuz;

- тактика – подготовка ресурсов;
- техника – подготовка необходимых средств.

Подготавливает необходимые ресурсы:

- тактика – первоначальный доступ;
- техника – T1190 «Недостатки в общедоступном приложении».

На сервере WebPortal2 находится сайт на WpDiscuz CMS, на котором установлен плагин WpDiscuz, уязвимость которого позволяет получить RCE.

После предыдущих уровней злоумышленник решает проверить уязвимость плагина wpDiscuz для версий 7.0.0 – 7.0.4, получая metersrpretter сессию, заменяет ссылку на скачивание какого-либо файла на reverseshell, ожидая скачивания и запуска этого файла пользователем;

- тактика – выполнение;

- техники – T1204.001 Вредоносная ссылка / T1204.002 Вредоносный файл.

Пользователь скачивает и запускает вредоносный файл;

- тактика – закрепление;
- техника – T1136.002 «Доменная учетная запись (техника)».

Получение доступа к AD.

На рис. 2 представлен сегмент сети с действия злоумышленника.

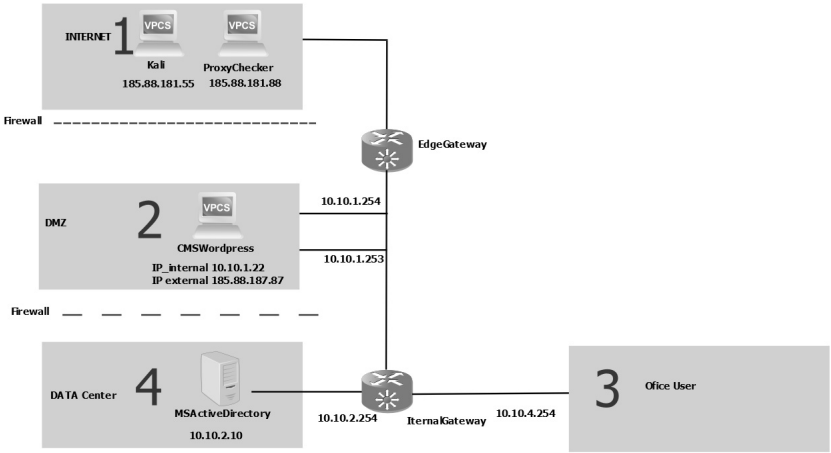


Рис. 2. Сегмент ЛВС с последовательностью действий злоумышленника

2.2. ПЕРЕЧЕНЬ УЯЗВИМОСТЕЙ И СПОСОБЫ ИХ ДЕТЕКТИРОВАНИЯ

Исходя из описания сценария были определены следующие уязвимости и их последствия:

- wpDiscuz (идентификационный номер CVE-2020-24186 в соответствии с базой данных общеизвестных уязвимостей CVE);
- Zerologon (идентификационный номер CVE-2020-1472 в соответствии с базой данных общеизвестных уязвимостей CVE);
- последствие Wordpress Shell;
- последствие получения прав доступа.

В работе [14] предлагается алгоритм окрестности инцидента, который в дальнейшем будет использоваться для объяснения способов детектирования уязвимостей и который необходим для безопасности автоматизированных систем [15].

Обнаружение и нейтрализация wpDiscuz

У CMS WordPress есть множество плагинов; WpDiscuz – один из плагинов для создания комментариев. Он представляет собой систему для комментариев на базе Ajax, которая хранит сообщения в локальной базе данных. В версиях с 7.0.0 по 7.0.4 есть уязвимость FileUpload, которая позволяет получить RCE, если прикрепить любой файл (например, код на php) в поле для комментариев и загрузить на сервер. Сделать это можно без аутентификации. Детектирование эксплуатации уязвимости удаленного выполнения кода CVE-2020-24186 с помощью сетевого сенсора ViPNet IDS NS (рис. 3 и 4).

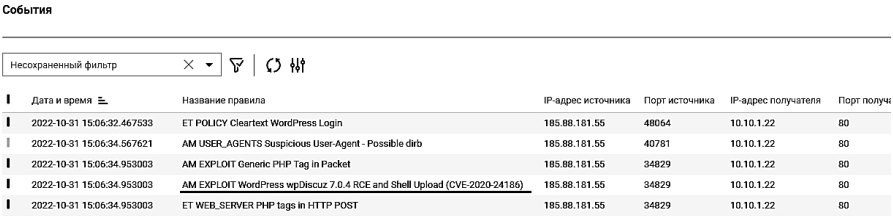


Рис. 3. Журнал событий сетевого сенсора ViPNet IDS NS

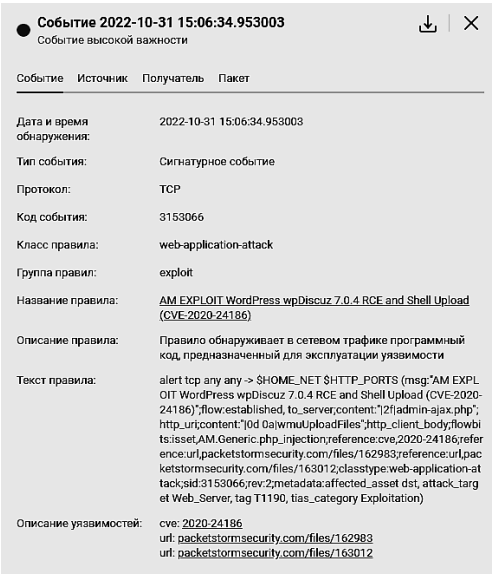


Рис. 4. Карточка события ИБ

Закрытие уязвимости можно осуществить следующими способами:

- отключение плагина wpDiscuz;
- обновление версии wpDiscuz до версии 7.0.5 и выше (при наличии интернета).

Обнаружение и нейтрализация payload

Данный payload заключается в том, что нарушитель устанавливает shell-сессию с уязвимой машиной.

Для того чтобы обнаружить эту полезную нагрузку, нужно проверить сокеты уязвимой машины на подключение к определенному порту машины нарушителя. Делается это при помощи утилиты ss. Следует просмотреть сокеты только нужного протокола (TCP) и отфильтровать данные (например, вывести только прослушиваемые tcp соединения):

$ ss -tn

Отображение информации о прослушиваемых TCP-соединениях уязвимой машины и завершении сессии с нарушителем показано ниже.

Для нейтрализации payload нужно также воспользоваться командой ss с правами привилегированного пользователя, используя ключ –K и соответствующий адрес, порт, что завершит сессию с нарушителем:

sudo ss –K dst 185.88.181.55 dport = 5764

Meterpreter-сессия с нарушителем завершена.

Обнаружение и нейтрализация Zerologon

Уязвимость в сервисе Netlogon позволяет обойти аутентификацию и сбросить пароль машинного аккаунта контроллера домена.

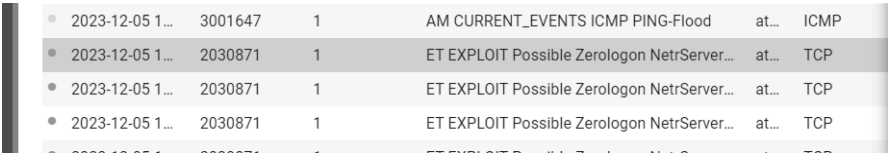
Уязвимость в сервисе Netlogon позволяет обойти аутентификацию и сбросить пароль машинного аккаунта контроллера домена. Эксплуатация этой уязвимости состоит из трех этапов:

- *отправка нулевых байтов.* Вместо отправки восьми случайных байтов атакующий отправляет нулевые байты до тех пор, пока сервер не примет одно из таких сообщений. Тем самым атакующий обходит процесс аутентификации и получает возможность совершать действия от имени контроллера домена;
- *отключение механизма RPC signing and sealing.* Атакующий отключает шифрование для того, чтобы сообщения отправлялись в открытом виде и атакующий мог использовать методы протокола MS-NRPC;
- *изменение пароля учетной записи контроллера домена.* Финальным шагом атаки является сброс пароля учетной записи контроллера домена.

Это открывает возможности для проведения атаки DCSync, которая направлена на получение существующих хэшей устройств в домене.

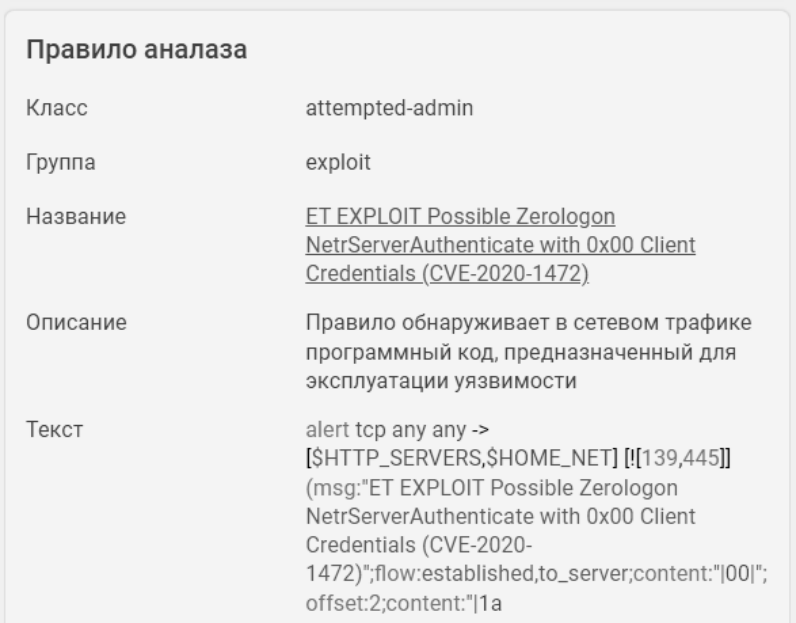
При атаке Zerologon в eventviewer генерируется событие 4742 (его можно найти во вкладке WindowsLogs>Security), в то время как при легитимной смене пароля контроллера домена будет сгенерировано два события: 4742 и 5823. В логах netlogon можно увидеть события, которые показывают успешный вход и смену пароля машинного аккаунта.

Детектирование эксплуатации уязвимости удаленного выполнения кода CVE-2020-1472 с помощью сетевого сенсора ViPNet IDS NS показано на рис. 5 и 6.



2023-12-05 1...	3001647	1	AM CURRENT_EVENTS ICMP PING-Flood	at...	ICMP
2023-12-05 1...	2030871	1	ET EXPLOIT Possible Zerologon NetrServer...	at...	TCP
2023-12-05 1...	2030871	1	ET EXPLOIT Possible Zerologon NetrServer...	at...	TCP
2023-12-05 1...	2030871	1	ET EXPLOIT Possible Zerologon NetrServer...	at...	TCP

Рис. 5. Журнал событий сетевого сенсора ViPNet IDS NS



Правило анализа

Класс	attempted-admin
Группа	exploit
Название	ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)
Описание	Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости
Текст	alert tcp any any -> [$HTTP_SERVERS,$HOME_NET] [![139,445]] (msg:"ET EXPLOIT Possible Zerologon NetrServerAuthenticate with 0x00 Client Credentials (CVE-2020-1472)";flow:established,to_server;content:"|00|"; offset:2;content:"|1a

Рис. 6. Карточка события ИБ

После успешной эксплуатации Zerologon происходит сброс пароля машинного аккаунта контроллера домена. В результате атакующему открывается возможность получить NTLM-хэши в домене и после этого с их помощью получить контроль над учетными записями в домене. Фактически лишение контроллера домена разрешения на запрос репликации делает атаку DCSync невозможной, что приведет к бесполезности уязвимости Zerologon.

Для изъятия вышеуказанного разрешения необходимо провести изменение настроек AD:

- включить в AD отображение расширенных опций (рис. 7);

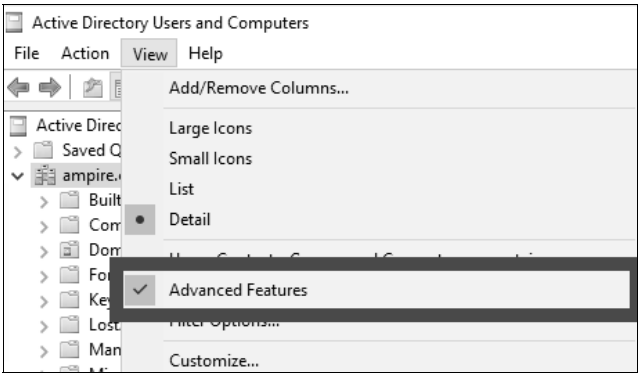


Рис. 7. Включение отображения расширенных опций

- изъять права ReplicatingDirectoryChanges;
- удалить нового привилегированного пользователя, который добавлен в Domain Admins. Факт добавления нового пользователя можно отследить в EventLog.

2.3. АПРОБАЦИЯ СЦЕНАРИЯ НА КИБЕРПОЛИГОНЕ

В апробации сценария приняли участие 5 вузов:

- ФГБОУ ВО «КНИТУ» (г. Казань).
- ФГБОУ ВО «КНИТУ – КАИ» (г. Казань).
- ФГБОУ ВО «КГЭУ» (г. Казань).
- ФГБОУ ВО «СамГТУ» (г. Самара).
- ФГБОУ ВО «СибГУ им. М.Ф. Решетнёва» (г. Красноярск).

По итогам прохождения сценария была составлена сводная таблица (см. таблицу).

Больше всего проблем возникло с уязвимостью Zerologon. Ее смогли закрыть только две команды из пяти, потратив на закрытие уязвимости около четырех часов. Уязвимость плагина Wordpress закрыли все команды, но только две команды устранили последствие Wordpress Shell. Также сложности возникли и с устранением последствия, связанного с получением доступа. По результатам киберучений можно сделать следующие выводы.

- Межвузовские киберучения позволяют студентам из разных вузов общаться и обучаться вместе, расширяя их знания и навыки.
- Участие в межвузовских киберучениих помогает студентам создавать профессиональные связи, которые могут быть полезны в будущей карьере.
- Межвузовские киберучения обучают студентов работать в команде и сотрудничать с другими людьми, что является важным навыком для будущих карьер.
- Остается открытым вопрос с технической поддержкой во время проведения киберучений. Во время проведения мероприятия существенных проблем не возникало, но некачественное обеспечение интернет-соединения, проблемы с программным обеспечением или аппаратным обеспечением могут помешать успешному проведению киберучений.
- В сравнении с традиционным обучением, киберучение может не обеспечивать полноценную онлайн-связь между преподавателем и учащимися.
- Так как география городов-участников разнообразна, участие в межвузовских киберучениях требовало адаптации к разным временным поясам и изменениям в учебном графике.

Результаты межвузовских киберучений

Вуз	Устранение уязвимости wpDiscuz, мин	Устранение уязвимости Zerologon, мин	Устранение последствия Wordpress Shell (да/нет)	Устранение уязвимости получения доступа (да/нет)
ФГБОУ ВО «КНИТУ»	169	0	нет	да
ФГБОУ ВО «КНИТУ – КАИ»	143	241	да	да
ФГБОУ ВО «КГЭУ»	161	225	нет	нет
ФГБОУ ВО «СамГТУ»	180	0	нет	нет
ФГБОУ ВО «СибГУ им. М.Ф. Решетнёва»	199	0	да	нет

ЗАКЛЮЧЕНИЕ

В сценарии действий злоумышленника используются различные тактики и приемы, включая активное сканирование, подготовку ресурсов, уязвимости в общедоступных приложениях, вредоносные ссылки и файлы, а также учетные записи пользователей домена. Представлены уязвимости и методы их обнаружения с упором на плагин wpDiscuz, Zerologon, а также последствия использования Wordpress Shell и получения несанкционированного доступа.

Уязвимость wpDiscuz (CVE-2020-24186) в плагине WordPress позволяет удаленно выполнять код (RCE) путем загрузки вредоносного файла без аутентификации. Эксплуатацию этой уязвимости можно обнаружить с помощью сетевых датчиков, таких как ViPNet IDS NS. Меры по снижению этой уязвимости включают отключение плагина wpDiscuz или обновление его до версии 7.0.5 или выше.

Обнаружение и нейтрализация полезной нагрузки включает в себя мониторинг сокетов уязвимой машины на предмет подключений к определенному порту, используемому злоумышленником.

Zerologon – еще одна уязвимость, позволяющая обойти аутентификацию и сбросить пароль учетной записи компьютера контроллера домена. Меры по смягчению последствий для Zerologon включают настройку параметров AD (в частности, дополнительных параметров) и отзыв прав Replicating Directory Changes.

В заключение отметим, что киберполигон на базе программного комплекса AMPIRE представляет собой платформу для изучения воздействия киберугроз. Благодаря реализации различных подсистем безопасности, включая мониторинг, контроль доступа, анализ сигнатур и ретроспективный анализ, эта линейка позволяет исследовать и устранять такие уязвимости, как wpDiscuz и Zerologon. Сценарное тестирование с участием вузов продемонстрировало эффективность комплекса при оценке времени, необходимого для смягчения уязвимостей и устранения последствий.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные тенденции на рынке информационной безопасности / А.В. Соломинский, В.А. Железин, А.Д. Миргородский, С.В. Краснобаев, Н.М. Колотилина // Вестник науки и образования. – 2023. – № 8 (139). – URL: https://cyberleninka.ru/article/n/aktualnye-tendentsii-na-rynke-informatsionnoy-bezopasnosti (дата обращения: 27.05.2024).

2. Моделирование вектора сетевых атак на локальную сеть с применением базы MITRE ATT&CK / А.Р. Касимова, В.В. Золотарев, Л.Х. Сафиуллина,

Д.И. Сабирова // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 4 (64). – С. 88–96. – DOI: 10.54398/20741707_2023_4_88. – EDN MPSCDH.

3. *Касимова А.Р., Сафиуллина Л.Х.* Использование цифровых двойников при построении системы безопасности предприятия // Международный форум «Kazan Digital Week – 2022»: сборник материалов / под общ. ред. Р.Н. Минниханова. – Казань, 2022. – Ч. 1. – С. 291–298.

4. *Шинкевич А.И., Надеждина М.Е., Сопин В.Ф.* Проектирование цифрового двойника системы организации производства // Стандарты и качество. – 2024. – № 4. – С. 94–99. – DOI: 10.35400/0038-9692-2024-4-197-23.

5. *Шинкевич А.И., Касимова А.Р., Алексеева А.А.* Использование цифровых двойников для экологизации химической промышленности // Известия Самарского научного центра Российской академии наук. – 2023. – Т. 25, № 4. – С. 87–94.

6. *Перухин М.Ю., Васильева М.Ю., Кадырова Г.К.* Цифровой двойник лаборатории систем управления химико-технологическими процессами // Современные наукоемкие технологии. – 2021. – № 6-1. – С. 84–90.

7. *Алексеева А.А., Касимова А.Р.* Перспективы применения цифровых двойников с целью экологизации производства // Комплексное изучение экосистем горных территорий: сборник материалов VI Кавказского международного экологического форума, Грозный, 20–21 октября 2023 года. – Грозный, 2023. – С. 16–19. – DOI: 10.36684/102-1-2023-16-19.

8. Цифровые двойники и цифровая трансформация предприятий ОПК / А.И. Боровков, Ю.А. Рябов, К.В. Кукушкин, В.М. Марусева, В.Ю. Кулемин // Вестник Восточно-Сибирской открытой академии. – 2019. – № 32. – С. 1–39.

9. *Шпак П.С., Сычева Е.Г., Меринская Е.Е.* Концепция цифровых двойников как современная тенденция цифровой экономики // Вестник Омского университета. Серия: Экономика. – 2020. – № 1. – С. 57–68.

10. *Хорзова И.С.* Применение возможностей киберполигона для подготовки и повышения квалификации специалистов по информационной безопасности // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. – Воронеж, 2021. – Т. 2. – С. 46–47.

11. Digital Twins and Cyber Security – solution or challenge? / D. Holmes, M. Papathanasaki, L. Maglaras, M.A. Ferrag, S. Nepal, H. Janicke // 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2021. – P. 1–8. – DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277.

12. Методическое пособие для обучаемого Ampire / Перспективный мониторинг. – URL: Локальный доступ.

13. Матрица ATT&CK. – URL: https://attack.mitre.org/ (accessed: 28.05.2024).

14. *Олейникова А.А., Золотарев В.В.* Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации // Известия ЮФУ. Технические науки. – 2023. – № 5 (235). – С. 66–81. – DOI: 10.18522/2311-3103-2023-5-66-81. – EDN KKJTDV.

15. Методика построения модели безопасности автоматизированных систем / В.Г. Жуков, М.Н. Жукова, В.В. Золотарев, И.В. Ковалев // Программные продукты и системы. – 2012. – № 2. – С. 70–74. – EDN OZYEVV.

Касимова Алина Ринадовна, старший преподаватель кафедры информационной безопасности ФГБОУ ВО «КНИТУ». Основное направление научных исследований – цифровые двойники в вопросах организации производства. E-mail: kasimovaar@corp.knrtu.ru

Воробьев Дмитрий Андреевич, ассистент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнёва. Область научных интересов – разработка автоматизированных сценариев моделирования атак информационной безопасности. E-mail: h1ppyfox1@gmail.com

Севрунов Александр Николаевич, ассистент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнёва. Область научных интересов – разработка автоматизированных сценариев моделирования атак информационной безопасности. E-mail: alexander.sevrunov@gmail.com

DOI: 10.17212/2782-2230-2024-2-9-24

Experience in conducting cyber exercises using a developed script *

A.R. Kasimova[1], D.A. Vorobiev[2], A.N. Sevrunov[3]

[1] *Kazan National Research Technological University, 68 Karl Marx Prospekt, Kazan, 420015, Russian Federation, senior lecturer of the Department of Information Security. E-mail: kasimovaar@corp.knrtu.ru*
[2] *Siberian State University of Science and Technology named after Academician M.F. Reshetnyova, 31 Avenue named after the newspaper "Krasnoyarsk Worker", Krasnoyarsk, 660037, Russian Federation, assistant of Department of Information Technology Security. E-mail: h1ppyfox1@gmail.com*
[3] *Siberian State University of Science and Technology named after Academician M.F. Reshetnyova, 31 Avenue named after the newspaper "Krasnoyarsk Worker", Krasnoyarsk, 660037, Russian Federation, assistant of Department of Information Technology Security. E-mail: alexander.sevrunov@gmail.com*

The threat of cyber attacks has become a serious problem for organizations, the solution of which also lies in the plane of modeling scenarios of possible attacks using digital twin technologies. A cyber polygon based on the AMPIRE software suite is used to study the impact of cyber threats. The attacker's scenario includes the use of various tactics and vulnerabilities, such as active scanning, provisioning, vulnerabilities in public applications, malicious links and files, and compromising domain user accounts. The vector of the malicious attack is related to the tactics, techniques and procedures of the Mitre ATT&CK matrix. Vulnerabilities include the wpDiscuz plugin, Zerologon, and the consequences of using Wordpress Shell and gaining unauthorized access. The ongoing intercollegiate cyber exercises have revealed strengths and weaknesses that need to be taken into account when conducting the following events. Scenario testing with the participation of universities showed the effectiveness of the complex in assessing the time required to close vulnerabilities and eliminate consequences. Implementation of different scenarios with specialized functionality at the cyber polygon makes it possible to form practical skills to prevent attacks on computer networks, and also allows you to analyze the situation, interact with other participating specialists.

Keywords: cyber learning, digital twin, mitre att & ck, digital twin, cyber polygon, attack vector, simulation, LAN

REFERENCES

1. Solominsky A.V., Zhelezin V.A., Mirgorodsky A.D., Krasnobaev S.V. Aktual'nye tendentsii na rynke informatsionnoi bezopasnosti [Current trends in the information security market]. *Vestnik nauki i obrazovaniya = Herald of Science and Education*, 2023, no. 8 (139). Available at: https://cyberleninka.ru/article/n/aktualnye-tendentsii-na-rynke-informatsionnoy-bezopasnosti (accessed 27.05.2024).

* *Received 20 March 2024.*

2. Kasimova R., Zolotarev V.V., Safiullina L.Kh., Sabirova D.I. Modelirovanie vektora setevykh atak na lokal'nuyu set' s primeneniem bazy MITRE ATT&CK [Modeling the network attack vector on a local network using the MITER ATT&CK]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2023, no. 4 (64), pp. 88–96. DOI: 10.54398/20741707_2023_4_88.

3. Kasimova A.R., Safiullina L.Kh. [Use of digital twins in building the security system of the enterprise]. *Mezhdunarodnyi forum «Kazan Digital Week – 2022»* [Proceedings of the International forum "Kazan Digital Week – 2022"]. Kazan, 2022, pt. 1, pp. 291–298. (In Russian).

4. Shinkevich A.I., Nadezhdina M.E., Sopin V.F. Proektirovanie tsifrovogo dvoinika sistemy organizatsii proizvodstva [Designing a digital twin for a production organization system]. *Standarty i kachestvo = Standards and Quality*, 2024, no. 4, pp. 94–99. DOI: 10.35400/0038-9692-2024-4-197-23.

5. Shinkevich A.I., Kasimova A.R., Alekseeva A.A. Ispol'zovanie tsifrovykh dvoinikov dlya ekologizatsii khimicheskoi promyshlennosti [Use digital twins for greening the chemical industry]. *Izvestiya Samarskogo nauchnogo tsentra Rossiiskoi akademii nauk = Izvestia of Samara Scientific Center of the Russian Academy of Sciences*, 2023, vol. 25, no. 4, pp. 87–94.

6. Perukhin M.Yu., Vasileva M.Yu., Kadyrova G.K. Tsifrovoi dvoinik laboratorii sistem upravleniya khimiko-tekhnologicheskimi protsessami [Digital twin of the laboratory of control systems of chemical-technological processes]. *Sovremennye naukoemkie tekhnologii = Modern High Technologies*, 2021, no. 6-1, pp. 84–90. (In Russian).

7. Alekseeva A.A., Kasimova A.R. [Prospects for the application of digital twins with the purpose of greening production]. *Kompleksnoe izuchenie ekosistem gornykh territorii* [Comprehensive study of ecosystems in mountain areas]. Collection of materials from the VI Caucasian International Environmental Forum, Groznyi, 2023, pp. 16–19. DOI: 10.36684/102-1-2023-16-19. (In Russian).

8. Borovkov A.I., Ryabov Yu.A., Kukushkin K.V., Maruseva V.M., Kulemin V.Yu. Tsifrovye dvoiniki i tsifrovaya transformatsiya predpriyatii OPK [Digital twins and digital transformation of defense industry enterprises]. *Vestnik Vostochno-Sibirskoi otkrytoi akademii*, 2019, no. 32, pp. 1–39. (In Russian).

9. Shpak P.S., Sycheva E.G., Merinskaya E.E. Kontseptsiya tsifrovykh dvoinikov kak sovremennaya tendentsiya tsifrovoi ekonomiki [The concept of digital twins as a modern trend of digital economy]. *Vestnik Omskogo universiteta. Seriya: Ekonomika = Herald of Omsk University. Series "Economics"*, 2020, no. 1, pp. 57–68.

10. Khorzova I.S. [Application of cyber polygon capabilities for training and advanced training of information security specialists]. *Aktual'nye voprosy eksplu-*

atatsii sistem okhrany i zashchishchennykh telekommunikatsionnykh sistem [Current issues of operation of security systems and secure telecommunications systems]. Voronezh, 2021, vol. 2, pp. 46–47. (In Russian).

11. Holmes D., Papathanasaki M., Maglaras L., Ferrag M.A., Nepal S., Janicke H. Digital Twins and Cyber Security – solution or challenge ? *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 2021, pp. 1–8. DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277.

12. *Methodological support for the general Empire*. Perspective monitoring. Available at: Local access.

13. ATT&CK Matrix. Available at: https://attack.mitre.org/ (accessed 28.05.2024).

14. Oleynikova A.A., Zolotarev V.V. Kontseptsiya upravleniya informatsionnoi bez-opasnost'yu na osnove tsikla nepreryvnogo detektirovaniya i reagirovaniya na intsidenty bezopasnosti informatsii [The concept of information security management based on a cycle of information security incidents continuous detection and response]. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering sciences*, 2023, no. 5 (235), pp. 66–81. DOI: 10.18522/2311-3103-2023-5-66-81.

15. Zhukov V.G., Zhukova M.N., Zolotarev V.V., Kovalev I.V. Metodika postroeniya modeli bezopasnosti avtomatizirovannykh sistem [Method of construction the security model of automated systems]. *Programmnye produkty i sistemy = Software and Systems*, 2012, no. 2, pp. 70–74.

Для цитирования:

Касимова А.Р., *Воробьев Д.А.*, *Севрунов А.Н.* Опыт проведения киберучений с использованием разработанного сценария // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 9–24. – DOI: 10.17212/2782-2230-2024-2-9-24.

For citation:

Kasimova A.R, Vorobiev D.A., Sevrunov A.N. Opyt provedeniya kiberuchenii s ispol'zovaniem razrabotannogo stsenariya [Experience in conducting cyber exercises using a developed script]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 9–24. DOI: 10.17212/2782-2230-2024-2-9-24.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 25–54

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-25-54

ОТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ К НАЦИОНАЛЬНОЙ: ПРОТИВОБОРСТВО IT-КОМПАНИЙ США И КНР*

Ю.Ю. ПЕТРУНИН[1], В.В. БУХАРИН[2]

[1] *119991, РФ, г. Москва, Ломоносовский проспект, 27, корпус 4, Московский государственный университет имени М.В. Ломоносова, доктор философских наук, профессор, заведующий кафедрой «Математические методы и информационные технологии в управлении». E-mail: petrunin@spa.msu.ru*

[2] *119991, РФ, г. Москва, Ломоносовский проспект, 27, корпус 4, Московский государственный университет имени М.В. Ломоносова, кандидат исторических наук, доцент кафедры «Математические методы и информационные технологии в управлении». E-mail: bukharin@spa.msu.ru*

В статье исследуются отдельные аспекты деятельности крупных IT-компаний, тесно связанные с проблемой информационной безопасности, обеспечения цифрового суверенитета как основы национальной безопасности. Особое внимание уделено борьбе транснациональных IT-корпораций США и КНР за альтернативные рынки сбыта, а также ряду ограничений, налагаемых на них законами иностранных государств. Основываясь на исследовании официальных документов американских и китайских государственных органов и IT-корпораций, а также материалов СМИ, авторы приходят к выводу, что геополитические интересы США и КНР соприкасаются с целями крупного бизнеса и вынуждают правительства прибегать к различного рода запретам и протекционистским мерам. IT-корпорации США и Китая, разработчики мессенджеров и социальных сетей уделяют недостаточно внимания вопросам информационной безопасности своих клиентов.

Ключевые слова: информационная безопасность, IT-корпорации, национальная безопасность, информационная война, цифровой суверенитет, Microsoft, Google, ByteDance, TikTok, WeChat, WhatsApp, Zoom, кибербезопасность

* Статья получена 16 мая 2024 г.

ВВЕДЕНИЕ

В современном мире влияние транснациональных компаний на национальные государства многократно возросло. Геополитические интересы США и КНР сталкиваются и переплетаются с целями крупного бизнеса. Наиболее ярко это проявляется в чрезвычайно быстро развивающейся IT-сфере. Деятельность крупных технологических компаний, обладающих огромными массивами данных своих клиентов и ресурсами для продвижения собственных интересов, выносит на повестку дня вопросы обеспечения информационной безопасности, влияния корпорации на национальную безопасность государства и их участия в информационных войнах. В рамках настоящей публикации предпринята попытка исследовать деятельность наиболее крупных корпораций IT-сферы США и Китая, разработчиков и владельцев мессенджеров, социальных сетей, что свидетельствует о новизне представленного исследования. В качестве методологической основы изучения этой проблемы были использованы принципы объективности и историзма, реализованные при анализе деятельности IT-компаний США и Китая. В соответствии с этими принципами был изучен широкий круг источников, среди которых наибольшее значение имели официальные документы американских и китайских корпораций, нормативно-правовые акты США и КНР, документы Министерства финансов США, Федеральной торговой комиссии США, Конгресса и Сената США, Министерства общественной безопасности КНР, Государственной канцелярии интернет-информации КНР, материалы американских и китайских СМИ, в том числе официального журнала Федерального правительства США Federal Register.

В отечественной и зарубежной историографии нет специальных работ, посвященных этой теме. Исследователи сосредоточили внимание на таких тематически близких проблемах, как информационный, цифровой и киберсуверенитет [1, 2], на различных аспектах национальной безопасности, геополитическом противостоянии США и КНР [3, 4], информационной войне [5], политике кибербезопасности [6–8], регулировании сети Интернет [9], а также отдельных вопросах кибербезопасности продуктов IT-корпораций [10].

ОСНОВНАЯ ЧАСТЬ

Информационная война – явление достаточно сложное и многогранное. Она может вестись как между блоками государств или отдельными странами, так и на уровне бизнеса, компаний. Цели информационных войн также могут очень сильно отличаться: от решения конкретных бизнес-задач до глобального доминирования в системе международных отношений, фор-

мирования однополярного мира. Исследование участия IT-корпораций в информационных войнах [5] представляет особый интерес, поскольку охватывает, по сути, все уровни, весь спектр проблем. В феврале 2019 года в разгар торговой войны между Соединенными Штатами Америки и Китайской Народной Республикой началась информационная война против социальной сети для обмена короткими видео в TikTok, принадлежащей пекинской компании ByteDance. США объявили TikTok угрозой национальной безопасности. Компания ByteDance была оштрафована Федеральной торговой комиссией (FTC) США. Одним из первых обвинений, выдвинутых в адрес TikTok со стороны американских политиков и бизнесменов, был сбор информации о пользователях – детях до 13 лет. На официальном сайте Федеральной торговой комиссии 27 февраля 2019 года было опубликовано заявление, что TikTok согласилась заплатить 5,7 млн долл. в целях урегулирования ситуации [11].

Юридическим продолжением конфликта между США и Китаем в информационной сфере стал опубликованный в августе 2020 года указ Президента США Дональда Трампа (2017–2021), предписывающий американским фирмам прекратить бизнес-сотрудничество с мобильной коммуникационной системой WeChat [12], разработанной компанией Tencent. Приложение WeChat используется во всём мире. Трамп обвинил WeChat в сборе «огромных массивов» личных данных пользователей, что, по его мнению, являлось угрозой безопасности американцев. Китайское пользователи WeChat расценили блокировку приложения, являющегося ярким примером технологических инноваций в Китае, как нападение на «свою культуру, свой народ» и государство. В ответ на решение Трампа Министерство иностранных дел Китая обвинило США в использовании проблемы национальной безопасности в качестве прикрытия для осуществления гегемонии. Действия президента США нанесли серьезный удар не только по крупной китайской IT-корпорации, но и повлияли на общественное мнение в Китае. Аудитория этого приложения насчитывает миллиард пользователей. WeChat – не только платформа социальных сетей, но и инструмент для решения множества повседневных задач, таких как покупки, игры, знакомства людей и др. Популярность приложения, по мнению ряда экспертов, связана с аналогичным запретом в Китае многих западных платформ, где с 2003 года в рамках проекта «Золотой щит» или «Великий китайский файрвол» [13] начали осуществлять фильтрацию содержимого интернета.

Одной из наиболее крупных западных корпораций, столкнувшихся с юридическими ограничениями, направленными на поддержку китайской информационной безопасности и информационного суверенитета [2], стала американская транснациональная корпорация Google, которая пыталась про-

никнуть на китайский IT-рынок. В 2006 году корпорация объявила, что она запустит китайские версии своих поисковых и новостных веб-сайтов, которые будут подвергать цензуре материалы в соответствии с законами КНР. «Google.cn будет соблюдать местные китайские законы и правила» [14], – говорилось в заявлении. «Решая, как лучше всего подойти к китайскому – или любому другому – рынку, мы должны сбалансировать наши обязательства по удовлетворению интересов пользователей, расширению доступа к информации и реагированию на местные условия» [14], – подчеркивал Google.

Подобным образом поступили и другие IT-корпорации. Например, Microsoft удалила блоги и блокировала запросы пользователей со словами «независимость Тайваня», «Тибет», «Далай-лама», «Фалуньгун», «терроризм» и «резня» на платформе для создания онлайн-журналов и блогов MSN Spaces [15], сославшись на свою политику соблюдения «местных законов».

Поисковая система Bing, разработанная и принадлежавшая Microsoft, в 2009 году не только осуществляла цензурированные поисковые запросы в Китае, но и, как обнаружил блогер портала New York Times Николас Кристоф, цензурировала все поисковые запросы, в которых использовались упрощенные китайские иероглифы, чаще всего применяемые в материковом Китае, в Сингапуре и среди студентов, изучающих китайский язык в других странах. По его мнению, эта «самоцензура», превзошла аналогичные действия корпорации Google. Политика Google заключалась в том, чтобы отображать результаты поиска на Google.com без цензуры в любой точке мира вне зависимости от того, используется ли китайский язык, но цензурировать результаты поиска на сайте google.cn после выхода серии публикаций этого блогера компания Microsoft признала наличие проблемы, но отрицала преднамеренность [16] своих действий. В 2010 году googl.com в Китае был заблокирован и американская корпорация вынуждена была уйти с китайского рынка.

В данный период ограничения в Китае были введены в отношении социальной сети Facebook, принадлежавшей корпорации Facebook (признана в России экстремистской организацией и запрещена), которая после ребрендинга 2021 года стала называться Meta Platforms (признана в России экстремистской организацией и запрещена) [17]. Социальная сеть была заблокирована в КНР после июльских беспорядков 2009 года в Урумчи в связи с тем, что активисты движения за независимость Синьцзяна использовали Facebook как часть своей коммуникационной сети. Facebook отрицал предоставление информации активистам [18]. В 2014 году в Китае была заблокирована социальная сеть Instagram (признана в России экстремистской организацией и запрещена), также принадлежащая компании Meta. Ее блокировку связывают с демонстрациями в Гонконге против политики китайских властей, с так

называемой «революцией зонтиков». Местные жители выкладывали в социальную сеть видео- и фотоматериалы, на которых были запечатлены столкновения протестующих с полицией. В отдельных китайских СМИ была опубликована информация о прекращении работы Instagram в КНР, однако о реальных причинах блокировки и протестах не сообщалось [19]. Примечательно, что эта транснациональная корпорация была заинтересована в освоении китайского рынка IT. Согласно информации, опубликованной в The New York Times, Facebook в 2015 году заблокировал около 55 000 единиц контента примерно в 20 странах [20]. Непосредственно для Китая, сообщалось в газете, разрабатывалось дополнительное программное обеспечение, позволяющее осуществлять более глубокую фильтрацию контента, включая новостные ленты. Автор статьи предположил, что данное программное обеспечение будет доступно партнерской китайской компании, которая получит «полный контроль над тем, должны ли эти сообщения отображаться в лентах пользователей» [20]. Официального комментария относительно планов Facebook не последовало.

Важно отметить, что 27 декабря 2015 года был принят «Закон о противодействии терроризму Китайской Народной Республики», в рамках которого ужесточался контроль за иностранными средствами массовой информации [21]. Согласно данному закону поставщики интернет-услуг и операторы связи должны предоставить технические интерфейсы, дешифрование и другую поддержку правоохранительным органам для борьбы с террористической деятельностью в соответствии с законодательством КНР. В законе также предусматривались меры по контролю над содержанием китайского интернет-трафика. Еще одним шагом Китая, направленным на укрепление национальной безопасности [8] в целом и информационной в частности, стал опубликованный 7 ноября 2016 года «Закон о кибербезопасности Китайской Народной Республики» [22]. Важно отметить, что среди положений этого закона были зафиксированы новые правила хранения данных операторами критической информационной инфраструктуры. Согласно статье 37 личная информация или важные данные должны храниться на территории материкового Китая. Несмотря на то что закон предполагал возможность передачи данных за рубеж («в связи с требованиями бизнеса»), этот алгоритм в законе не был детализирован. В документе отсутствовало также четкое определение «критически важной информационной инфраструктуры». В законе отмечалось, что в некоторых случаях сбор данных может осуществляться только с разрешения правительства Китая. Закон неоднократно подвергался критике со стороны западной прессы. По мнению некоторых американских аналитиков, «Закон о кибербезопасности Китайской Народной Республики» может быть «уязвим» для злоупотребления со стороны китайского правительства. Кроме того, ино-

странные фирмы оказались в неравном положении с китайскими и обязаны нести дополнительные финансовые издержи.

The Wall Street Journal в начале 2017 года отмечала, что Facebook предпринял множество попыток для возвращения в Китай. Однако, по мнению авторов статьи, некоторое время казалось, что шансы вернуться на китайский рынок IT изменились к лучшему, когда власти Пекина предоставили Facebook лицензию, позволяющую открыть представительство в двух офисных башнях в столице [23]. Вместе с тем можно сделать вывод, что подобные «успехи» были мнимыми, поскольку разрешение было выдано на очень короткий срок (3 месяца) и корпорация Facebook им не воспользовалась.

Важно отметить, что Китай попытался также заблокировать возможные пути обхода введенных ограничений. Считается, что наиболее распространенным способом преодоления блокировки для доступа к западным мессенджерам и соцсетям является использование технологии VPN (от англ. virtual private network – «виртуальная частная сеть») [24]. Согласно информации, опубликованной в американских и гонконгских СМИ, в марте 2016 года во время заседания высшего законодательного органа КНР «Всекитайского собрания народных представителей» в Пекине VPN-сервисы в Китае были заблокированы.

«Многие компании жаловались, что их платные VPN-сервисы не функционировали почти неделю» [25]. Министерство информации и технологий Китая объявило, что VPN-сервисы должны получить лицензию от регуляторов [26]. Подобные меры автоматически ограничили использование западных VPN-сервисов в Китае, сделав многие из них нелегальными. Необходимо отметить, что ограничения касались не самой технологии VPN, которая часто используется в корпоративном секторе, а VPN-анонимайзеров, применяемых во многих странах для обхода различных блокировок. Дальнейшая борьба с VPN продолжилась и в 2018 году, когда крупнейшие провайдеры страны China Mobile, China Unicom и China Telecom заблокировали доступ к VPN [25]. А 31 марта в Китае был введен полный запрет на использования VPN. Несмотря на то что ряд экспертов отмечали важность принятого закона, поставившего, по их мнению, окончательную точку в борьбе с использованием VPN для обхода ограничений, на момент его принятия многие сервисы уже были заблокированы [27].

Ограничения коснулись не только социальной сети Facebook, принадлежащей одноименной корпорации, но и приобретенного ею в 2014 году мессенджера WhatsApp. Он был заблокирован в 2017 году. По мнению газеты New York Times, это было связано с «усилением слежки в преддверии большого собрания Коммунистической партии» [28]. Отключение мессенджера для материкового Китая стало серьезным ударом для IT-гиганта. Незадолго до

этих событий исполнительный директор Facebook Марк Цукерберг настаивал на возвращении мессенджера на китайский рынок и интенсивно изучал китайский язык [29].

New York Times делала акцент на защищенность WhatsApp от контроля китайских цензоров. Действительно, в приложении присутствует функция так называемого сквозного шифрования. Однако утверждение, что владельцы Facebook не могут получить доступ к текстовым, голосовым и видеосообщениям, проходящим через их серверы, выглядит не вполне обоснованным, поскольку в том же году стало широко известно о наличии «бекдора»[1] в этом приложении, который позволяет компании подменить ключи шифрования и потребовать от приложения-отправителя повторно зашифровать все сообщения и отправить, используя новые ключи [30]. Когда подобная информация стала широко известна, то возник вопрос, насколько действия со стороны США правомочны. В ответ на запрос от сенатора Дж. Рона Уайдена [31] правительство США заявило, что не нуждается в судебном решении для осуществления слежки и может попросить технологическую компанию создать бэкдор в шифровании [10]. Правительство до настоящего времени руководствовалось разделом 702 «Закона о надзоре за внешней разведкой» [32] для осуществления основной части своих операций по сбору разведданных и наблюдению. Применение полномочий, предоставляемых этим законом, давало право правительству требовать от технологических компаний специально обходить шифрование в своих продуктах.

Подобный способ обхода шифрования был некогда встроен и в принадлежащий Microsoft мессенджер Skype, а также не стоит забывать о программе PRISM [33], к которой присоседилась Microsoft еще в 2011 году [34]. Следует отметить, что сама компания до сих пор отрицает наличие свободного доступа со стороны спецслужб к информации своих серверов благодаря данной программе. По утверждению компании Microsoft, PRISM [1, с. 86] – «это не добровольная программа, а внутренняя правительственная компьютерная система для обработки целевых данных, собранных в соответствии с действующими законами» [35]. Microsoft также приводит заявление директора национальной разведки, который, поясняя ситуацию с PRISM, ссылался на уже упомянутый раздел 702 «Закона о надзоре за внешней разведкой» [36].

В актуальном лицензионном соглашении WhatsApp (дата вступления в силу: 4 января 2021 г.) сказано, что, «являясь одной из компаний Meta, WhatsApp получает информацию от других компаний Meta и предоставляет информацию другим компаниям Meta» [37]. На практике это означает, что Facebook получит

[1] От англ. back door – «черный ход» или «тайный ход», позволяющий получить несанкционированный доступ к данным.

доступ к номерам телефонов, сведениям о транзакциях и IP-адресам пользователей. Следовательно, полученные данные могут быть использованы не только в коммерческих интересах компании и переданы третьим лица, но и в информационной войне, создавая угрозу национальной безопасности.

Социальная сеть Facebook уже давно стала площадкой информационной войны. По словам В.Б. Вехова, эксперта в области информационной безопасности, профессора кафедры юриспруденции интеллектуальной собственности и судебной экспертизы МГТУ им. Баумана, «Facebook изначально являлся не только коммерческим проектом, но и проектом, направленным на ведение информвойны, поскольку финансировался за счет денежных средств фонда Сороса. Соответственно, в условиях, когда необходимо применять один из элементов информационного оружия, он и был применен» [38]. М.Г. Делягин – доктор экономических наук, депутат ГД РФ, член научного совета при Совете Безопасности РФ – отметил, что «поднимал вопрос о необходимости блокировки Facebook, откровенно русофобского политического инструмента» [39]. Проблема заключается не только в том, что США используют Facebook в информационной войне против государств (таких как РФ или КНР) и организуют с его помощью цветные революции, но и подвергают опасности персональные данные каждого пользователя, конкретного человека. При этом США позиционируют себя как главного в мире защитника интересов и свободы личности.

Несмотря на тот факт, что наиболее известной иллюстрацией подобной угрозы является скандал, связанный с компанией Cambridge Analytica, которая использовала данные более 50 млн пользователей Facebook, чтобы влиять на избирателей перед голосованием по Brexit, следует прежде всего обратить внимание на события, произошедшие в 2021 году, являющиеся примером использования исключительно технических уязвимостей. Так, 3 апреля 2021 года, согласно информации, опубликованной на страницах Insider, 533 млн телефонных номеров и личных данных пользователей Facebook «утекли» в Интернет [40]. Подобные угрозы невозможно ликвидировать запретом зарубежных компаний, однако дополнительный контроль и аудит безопасности может уменьшить вероятность их возникновения. Несмотря на масштаб проблемы, противодействие подобным угрозам представляется достаточно сложной задачей, особенно если учитывать, что коммерческий интерес в деятельности социальных сетей превалирует над интересами национальной безопасности. Случаи, аналогичные описанному на страницах Insider, представляют для владельцев соцсетей исключительно репутационные риски, но не оказывают достаточно серьезного влияния на финансовое состояние владеющих ими корпораций. Среди стран, пострадавших от утечки, только в Ирландии была предпринята попытка применить экономические инстру-

менты. Так, в середине апреля 2021 года ирландская юридическая фирма Digital Rights Ireland (DRI) объявила о подаче иска против Facebook за утечки данных миллионов пользователей социальной сети. Ирландская фирма предложила всем пострадавшим присоединиться к иску против цифрового гиганта [41]. С этой целью была создана интернет-страница, позволяющая зарегистрироваться и принять участие в иске [42].

Еще один интересный случай противоборства в сети Интернет связан с компанией Zoom Video Communications. Zoom (приложение для видеоконференц-связи, значительно увеличило свою аудиторию в 2020 году во время введения карантина (пандемии COVID-19)) использовали и продолжают использовать миллионы людей для работы и проведения общественных мероприятий. Например, в марте 2020 года премьер-министр Великобритании Борис Джонсон опубликовал на своей странице в соцсети Twitter фотографию, на которой он председательствовал на заседании Кабинета министров через приложение [43].

Компания Zoom Video Communications основана выходцем из Китая Эриком Юань и базируется в США. Есть основание предполагать, что приложение Zoom было разработано тремя компаниями в Китае, каждая из которых имела название Ruanshi Software, две из них принадлежали непосредственно компании Zoom, третья – компании American Cloud Video Software Technology Co., Ltd. [44]. Косвенно приведенные факты легко подтвердить, если обратить внимание на данные регистрационной формы S-1[2], согласно которой на конец января 2019 года в Китае штат программистов Zoom составлял 500 человек [45]. Согласно документам американской Комиссии по ценным бумагам, в 2020 году Zoom нанимал через свои филиалы в Китае не менее 700 сотрудников, которые занимались «исследованиями и разработками» [46]. Zoom неоднократно блокировал пользователей по запросу китайского правительства, а согласно официальному заявлению, опубликованному в июле 2020 года, Zoom разрабатывал технологию, которая позволила бы компании удалять или блокировать пользователя на основе их географического расположения по запросу местных властей, когда публикации пользователей являлись незаконными в их юрисдикции [47].

В сети в настоящее время распространилась непроверенная информация, что «Zoom подтвердил, что Zoom.us теперь доступен в Китае в дополнение к Zoom.com. Данные местных пользователей Китая будут храниться в центрах обработки данных Zoom, расположенных в Китае, и этим пользователям также потребуется ввести действительный номер мобильного телефона для

[2] Форма S-1 SEC – первоначальная регистрационная форма для новых ценных бумаг, требуемая Комиссией по ценным бумагам и биржам США.

использования Zoom» [48]. По сообщениям, опубликованным в «Сообществе Zoom» [49], можно сделать вывод, что международная версия сайта на момент публикации настоящей статьи была заблокирована. Официальная служба поддержки приложения на сообщения пользователей о проблемах с использованием Zoom в КНР не отвечала. Проанализировав информацию, опубликованную в «Сообществе Zoom», и публикации в СМИ, можно сделать вывод, что пользователи имели возможность присоединяться к конференции, но им была недоступна функция «создать конференцию». Возможность создавать конференции существовала только у владельцев «премиальной» подписки, которую было возможно приобрести у местного дилера. Все китайские пользователи могли присоединиться к любой конференции Zoom в Гонконге и за рубежом, а также в материковом Китае, используя URL-адрес приглашения или идентификатор конференции. (Пользователям из материкового Китая необходимо предоставить номер телефона, чтобы подтвердить свою личность и присоединиться к собранию.)

Введение жестких ограничений на использование зарубежных мессенджеров полностью согласуется с информационной политикой КНР, направленной на защиту информационной безопасности. Важно отметить, что даже китайские WeChat, Weibo, Baidu Tieba не избежали проверки на соблюдение «закона о контенте» [50]. Информация о проведении расследования в отношении упомянутых компаний была опубликована на официальном сайте Администрации киберпространства Китая (CAC) – государственного органа, контролирующего содержание китайского сегмента интернета [51]. Представляется важным упомянуть «Положение о надзоре и проверке интернет-безопасности органами общественной безопасности», которое было принято Министерством общественной безопасности КНР 5 сентября 2018 года (обнародовано и вступило в силу 1 ноября 2018 г.). Этот документ наделил правоохранительные органы полномочиями на доступ (в том числе удаленный) и копирование данных, имеющих отношение к кибербезопасности [52].

На момент выхода приложение Zoom имело серьезные недостатки в системе безопасности, включая уязвимость, которая позволяла злоумышленнику удалять участников собраний, подделывать сообщения от пользователей и использовать общие экраны. Это вызвало вопрос: насколько безопасно его использовать для правительственных заседаний. В настоящей статье мы не ставим своей задачей проанализировать уязвимости приложения, а рекомендуем читателю обратиться к тематическим публикациям. Например, к статье в журнале Forbes, опубликованной в 2020 году под названием «Все “дыры” Zoom: чем рискуют пользователи самого популярного сервиса видеоконференций эпохи карантина» [53]. Популярность Zoom сделала его лакомым объектом как для хакеров, так и для государственных структур США. Как и мно-

гие западные ресурсы, Zoom небезопасен и может быть использован не только хакерами, но и спецслужбами в глобальном информационном противостоянии. Даже если не вдаваться в конспирологические теории, забыть на какой-то момент про информационные войны, а просто внимательно изучить «заявление о конфиденциальности» [54], то можно заметить, что Zoom продолжает передавать информацию рекламным партнерам (например, Google Ads и Google Analytics), а реальная защита информации обеспечивается исключительно для госучреждений США, поскольку их данные размещены на территории США в отдельном облаке, сертифицированном в рамках Федеральной программы управления рисками и авторизацией (FedRAMP).

В документации Zoom также присутствует ряд неясных заявлений о шифровании. В некоторых документах и приложении Zoom говорится о том, что платформа в настоящее время использует сквозное (E2E) шифрование [55], однако согласно официальному пояснению, опубликованному в блоге компании Zoom, корпорация дает собственную трактовку данного термина, далекую от общепринятой [44]. Важно отметить, что использование «сквозного шифрования», согласно инструкции [56], требует дополнительных манипуляций от самого пользователя. Таким образом, можно сделать вывод, что сквозное шифрование может оказаться не более чем маркетинговым ходом.

Действия Китая по отношению к американским корпорациям не являются уникальными, как это часто изображается в западных СМИ. В той или иной степени к подобным мерам прибегали и другие страны. Так, Facebook кроме Китая заблокировали Северная Корея, Мьянма, Иран, Куба, Россия, Туркменистан [9].

В 2020 году правительство США объявило, что рассматривает возможность запрета китайской социальной сети TikTok, принадлежащей ByteDance. Министерство обороны и Пентагон запретили использовать данную социальную сеть военным [57]. Примечательно, что ранее военные США размещали в соцсети рекламный контент для привлечения в свои ряды новых рекрутов [58]. В августе Трамп подписал указы [59], запрещавшие американским компаниям заключать какие-либо сделки с китайской компанией ByteDance, вынуждая компанию продать TikTok. В ответ на действия Трампа 24 августа 2020 года в окружной суд Центрального округа Калифорнии был подан иск, в котором утверждалось, что указ был мотивирован стремлением президента укрепить свою поддержку на выборах благодаря протекционистским мерам, направленным против Китая [60]. В иске также подчеркивалось, что TikTok и ByteDance были лишены права на справедливое процессуальное обеспечение в соответствии с пятой поправкой, которая распространяется на иностранные и местные компании;

что президентский указ не предоставил доказательств реальной угрозы, исходящей от TikTok, для безопасности страны, а также достаточного обоснования для данного запрета. TikTok протестовал против применения устаревшей декларации о чрезвычайной ситуации от мая 2019 года относительно «обеспечения цепочки поставок информационных и коммуникационных технологий и услуг». В иске утверждалось, что предполагаемая угроза для национальной безопасности, выявленная Комитетом по иностранным инвестициям США (CFIUS), была основана на устаревших данных и не учитывала предоставленные TikTok документы [61].

В 2020–2021 годах несколько крупных американских компаний рассматривали возможность приобретения как самого TikTok, так и технологий, используемых компанией ByteDance [62]. Корпорация Microsoft выразила намерение о приобретении алгоритма работы TikTok, а также некоторых других технологий, связанных с искусственным интеллектом. Согласно информации, опубликованной телеканалом CNBC, сумма обсуждаемой сделки могла составить от 20 до 30 млн долл. [63]. Несмотря на давление [3, с. 20] со стороны правительства США, ByteDance сохранила независимость, отказав американской компании [64].

Администрация президента Дж. Байдена 9 июня 2021 года издала указ «Защита конфиденциальных данных американцев от иностранных противников» («ЕО 14034») [65]. Документ отменил три указа, изданных администрацией Трампа, которые фактически запрещали использование некоторых китайских приложений в США, включая TikTok и WeChat. Несмотря на отмену этих законов, в документе было подчеркнуто, что в соответствии с «Указом 13873» [66] «Китайская Народная Республика, среди прочего, продолжает угрожать национальной безопасности, внешней политике и экономике Соединенных Штатов». Документ призвал федеральные агентства продолжить широкую проверку приложений, «принадлежащих или контролируемых иностранным противником» [66].

Законодатели США 13 декабря 2022 года представили в Конгресс проект закона, который запрещал использование TikTok и позволял вводить санкции против медиакомпаний, подконтрольных определенным странам. По мнению авторов, этот закон должен был защитить американцев от угрозы со стороны социальных сетей Китая, России и ряда других иностранных государств (или находящихся под их влиянием) [67]. Разработчиками закона являлись сенатор Марко Рубио (республиканец от штата Флорида), а также члены Палаты представителей Конгресса США Майк Галлахер (республиканец от штата Висконсин) и Раджа Кришнамурти (демократ от штата Иллинойс). Законодатели в качестве угрозы национальной безопасности отмечали, что по китайскому законодательству компания обязана предоставить эти приложения

Коммунистической партии Китая (КПК). В опубликованном пресс-релизе отмечалось, что «от директора ФБР до комиссаров FCC и экспертов по кибербезопасности все ясно дали понять о риске использования TikTok для слежки за гражданами США» [67]. Президент Джо Байден 30 декабря 2022 года подписал закон о запрете TikTok на «государственных устройствах». Закон запретил установку и использование TikTok на всех (с некоторыми исключениями) устройствах федерального правительства и государственных корпораций и предписывал удалить TikTok там, где он уже установлен [68]. Согласно информации, опубликованной телеканалом NBC, «администрация Байдена пригрозила потенциальным запретом популярного приложения для социальных сетей в США, если его китайские владельцы откажутся продавать свои доли в нем» [69]. Авторы репортажа также недвусмысленно намекнули, что именно позиция администрации Байдена стала причиной начатого 17 марта 2023 года ФБР и Министерством юстиции США официального расследования фактов шпионажа за американскими журналистами.

В начале марта 2023 года в Сенат США был представлен «Закон об ограничении» [70]. Законопроект требовал от федерального правительства принять меры по обнаружению и устранению угроз, исходящих из-за границы, в отношении продуктов и услуг в сфере информационно-коммуникационных технологий, таких как приложения для социальных сетей. В законопроекте было подчеркнуто, что «Министерство торговли должно выявлять, сдерживать, срывать, предотвращать, запрещать, расследовать и смягчать последствия транзакций, связанных с продуктами и услугами ИКТ, в которых любой иностранный противник (такой как Китай) имеет какой-либо интерес и которые представляют неоправданный или неприемлемый риск для национальной безопасности США или безопасности граждан США» [70]. Через год в США был принят «Закон о защите американцев от приложений, контролируемых иностранными противниками» (HR 7521) [71]. Из закона следовало, что если TikTok в течение полугода не сменит владельца и останется частью китайской компании ByteDance, то его заблокируют в США. Согласно информации, опубликованной в The Wall Street Journal, правительство Китая «сигнализировало» компании ByteDance, что предпочтет запрет в США продаже социальной сети [72].

ЗАКЛЮЧЕНИЕ

В современном мире происходит борьба транснациональных IT-компаний за альтернативные рынки сбыта, а также новых клиентов. Стратегия различных транснациональных компаний в IT-сфере имеет достаточно много общих

черт вне зависимости от страны происхождения бизнеса. Корпорации, стремясь максимизировать свою прибыль, пытаются всеми возможными способами потеснить конкурентов, достичь технологического преимущества [4]. Ради достижения этой цели они готовы мириться с некоторыми ограничениями, налагаемыми на них законами иностранных государств.

Как показывает проведенный анализ, корпорации уделяют недостаточно внимания вопросам информационной безопасности своих клиентов. Данные пользователей постоянно находятся в зоне риска. Важно отметить, что инциденты, связанные с утечкой персональных данных, происходят достаточно часто, однако материальный и репутационный ущерб для крупных компаний не является фатальным. Заявления ряда компаний о высокой степени защиты данных (например, об использовании сквозного шифрования) не в полной мере соответствуют действительности, часто являются маркетинговым ходом.

Правительства США и Китая прибегают к различного рода ограничениям и протекционистским мерам, оказывая поддержку собственному крупному бизнесу. Для США это коррелируется с защитой национальной безопасности, поскольку лидерство США, обеспечиваемое в IT-сфере крупными корпорациями, трактуется данной страной как основной способ обеспечения ее национальной безопасности. В погоне за глобальным доминированием США стремятся взять под свой контроль информационное пространство других государств.

США и Китай уделяют достаточно много внимания своей информационной безопасности, обеспечению цифрового суверенитета как основы национальной безопасности. В их подходе к решению этой задачи есть как общие черты, так и принципиальные различия. Оба государства активно внедряют информационно-коммуникационные технологии в социально-экономическую жизнь страны, но при этом стремятся ограничить доступ к данным своих граждан со стороны иностранных держав.

Принципиальные различия в подходе к обеспечению информационной безопасности между Соединенными Штатами Америки и Китаем касаются трех ключевых аспектов: свободы интернета, места и роли государства в области информационной безопасности, сотрудничества и обмена информацией [6] с другими странами и международными организациями в области кибербезопасности. США декларируют защиту прав граждан на свободный доступ к информации и свободу выражения мнения в сети. Такой подход объясняется доминированием американских IT-корпораций, контролируемых американским правительством и спецслужбами, в то время как в Китае интернет цензурируется и контролируется государством, что в значительной степени является ответом на внешние угрозы. Например, торго-

вая война с США стимулировала усиление информационного контроля в Китае. Обеспечение информационной безопасности в США в значительной степени возлагается на частный бизнес, коммерческие компании. В Китае государство играет центральную роль в контроле и регулировании информационной безопасности, а также принимает более строгие меры для мониторинга и контроля интернета. США активно сотрудничают с другими странами и международными организациями в области кибербезопасности. Китай также осуществляет сотрудничество, например, в рамках ООН или БРИКС [7], однако в менее широком формате в связи с особенностями политики контроля над информацией.

СПИСОК ЛИТЕРАТУРЫ

1. *Бухарин В.В.* Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. – 2016. – № 6 (51). – С. 76–91. – DOI: 10.24833/2071-8160-2016-6-51-76-91.

2. *Moore G.J.* Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies // Journal of Chinese Political Science. – 2023. – Vol. 28 (1). – P. 151–167. – DOI: 10.1007/s11366-022-09814-2.

3. *Цветкова Н., Сытник А.* Цифровое противостояние США и КНР: экономическое и политическое измерения // Мировая экономика и международные отношения. – 2023. – Т. 67, № 11. – С. 15–23. – DOI: 10.20542/0131-2227-2023-67-11-15-23.

4. *Гамза Л.А.* Технологическое противостояние США и Китая в Европе // Мировая экономика и международные отношения. – 2021. – Т. 65, № 7. – С. 98–105.

5. *Каткова Е.Ю., Юнюшкина А.С.* Китайские концепции и возможности в информационной войне: соперничество КНР и США в киберпространстве // Вестник РУДН. Серия: Всеобщая история. – 2022. – Т. 14, № 2. – С. 197–210. – DOI: 10.22363/2312-8127-2022-14-2-197-210.

6. *Julian N.* United States' and China's cybersecurity policies: collaboration or confrontation? // The Sigma Iota Rho (SIR) Journal of International Relations. – 2021. – January 24. – URL: https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation (accessed: 29.05.2024).

7. *Бухарин В.В.* Кибербезопасность БРИКС // Государственное управление Российской Федерации: повестка дня власти и общества. Материалы

XVI Международной конференции (31 мая – 02 июня 2018 г.). – М., 2019. – С. 552–559.

8. *Cheung T.M.* The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities // Journal of Cyber Policy. – 2018. – Vol. 3 (3). – P. 306–326. – DOI: 10.1080/23738871.2018.1556720.

9. *Курылев К.П., Пархитько Н.П., Смолик Н.Г.* Национальные режимы регулирования сети интернет в странах СНГ // Постсоветские исследования. – 2021. – Т. 4, № 8. – С. 705–718. – DOI: 10.24412/2618-7426-2021-8-705-718.

10. *Endeley R.E.* End-to-end encryption in messaging services and national security – case of Whatsapp messenger // Journal of Information Security. – 2018. – Vol. 9 (1). – P. 95–99. – DOI: 10.4236/jis.2018.91008.

11. Video social networking app Musical.ly agrees to settle FTC allegations that it violated children's privacy law // Federal Trade Commission. – 2019. – February 27. – URL: https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc (accessed: 29.05.2024).

12. *Zhaoyin F., Cheetham J.* Trump WeChat ban 'an unwelcome signal' for Chinese community // BBC. – 2020. – August 10. – URL: https://www.bbc.com/news/world-asia-china-53686507 (accessed: 09.01.2024).

13. *Shen X.* The story of China's Great Firewall, the world's most sophisticated censorship system // South China Morning Post. – 2019. – November 7. – URL: https://www.scmp.com/abacus/who-what/what/article/3089836/story-chinas-great-firewall-worlds-most-sophisticated (accessed: 29.05.2024).

14. *Mills E.* Google to censor China Web searches // CNET. – 2006. – January 25. – URL: https://www.cnet.com/news/google-to-censor-china-web-searches/ (accessed: 29.05.2024).

15. *Watts J.* Microsoft helps China to censor bloggers // The Guardian. – 2005. – June 15. – URL: https://www.theguardian.com/technology/2005/jun/15/newmedia.microsoft (accessed: 29.05.2024).

16. *Kristof N.* Microsoft and Chinese Censorship // The New York Times. – 2009. – June 24. – URL: https://archive.nytimes.com/kristof.blogs.nytimes.com/2009/06/24/microsoft-and-chinese-censorship/?searchResultPosition=6 (accessed: 29.05.2024).

17. Информация по делу № 02-2473/2022 // Официальный портал судов общей юрисдикции г. Москвы. – URL: https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35?participants=meta (дата обращения: 29.05.2024).

18. 80 pct of netizens agree China should punish Facebook // People's Daily Online. – 2009. – July 10. – URL: https://en.people.cn/90001/90776/90882/6697993.html (accessed: 01.08.2020).

19. *Коцар Ю., Бевза Д.* Протесты лишили Китай Instagram // Газета.Ru – 2014. – 29 сентября. – URL: https://www.gazeta.ru/tech/2014/09/29_a_6240045.shtml (дата обращения: 29.05.2024).

20. *Isaac M.* Facebook said to create censorship tool to get back into China // The New York Times. – 2016. – November 22. – URL: https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html (accessed: 29.05.2024).

21. Counter-Terrorism Law (as amended in 2018) // China Law Translate. – URL: https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/ (accessed: 29.05.2024).

22. *Creemers R., Webster G., Triolo P.* Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) / Stanford Cyber Policy Center. – URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (accessed: 29.05.2024).

23. *Abkowitz A., Seetharaman D., Dou E.* Facebook is trying everything to Re-Enter China – and it's not working // The Wall Street Journal. – 2017. – January 30. – URL: https://www.wsj.com/articles/mark-zuckerbergs-beijing-blues-1485791106 (accessed: 29.05.2024).

24. *Economy E.C.* The great firewall of China: Xi Jinping's internet shutdown // The Guardian. – 2018. – June 29. – URL: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown (accessed: 29.05.2024).

25. *Ye J.* China tightens Great Firewall by declaring unauthorised VPN services illegal // South China Morning Post. – 2017. – January 23. – URL: https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall (accessed: 29.05.2024).

26. How Web-connected is China? / ChinaPower. – URL: https://chinapower.csis.org/web-connectedness (accessed: 29.05.2024).

27. China's internet underground fights for its life // Bloomberg. – URL: https://www.bloomberg.com/news/articles/2018-03-01/china-s-internet-underground-fights-for-its-life (accessed: 29.05.2024).

28. *Bradsher K.* China blocks WhatsApp, broadening online censorship // The New York Times. – 2017. – September 25. – URL: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html (accessed: 29.05.2024).

29. *Mozur P.* China disrupts WhatsApp service in online clampdown // The New York Times. – 2017. – July 18. – URL: https://www.nytimes.com/2017/07/18/technology/whatsapp-facebook-china-internet.html (accessed: 29.05.2024).

30. WhatsApp design feature means some encrypted messages could be read by third party // The Guardian. – 2017. – January 13. – URL: https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages (accessed: 29.05.2024).

31. *Whittaker Z.* US says it doesn't need secret court's approval to ask for encryption backdoors // ZDNet. – 2017. – December 7. – URL: https://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors/ (accessed: 29.05.2024).

32. FISA questions (July 2017). Wyden's encryption backdoor question // Web archive. – URL: https://web.archive.org/web/20230106172742/https://www.documentcloud.org/documents/4320971-FISA-questions-July-2017.html (accessed: 29.05.2024).

33. *Gellman B., Lindeman T.* Inner workings of a top-secret spy program // Washington Post. – 2013. – June 29. – URL: https://web.archive.org/web/20170830105407/https://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/ (accessed: 29.05.2024).

34. Microsoft handed the NSA access to encrypted messages / G. Greenwald, E. MacAskill, L. Poitras, S. Ackerman, D. Rushe // The Guardian. – 2013. – July 12. – URL: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (accessed: 29.05.2024).

35. Microsoft. About our practices and your data – URL: https://blogs.microsoft.com/datalaw/our-practices/#did-participate-in-prism-program (accessed: 29.05.2024).

36. Facts on the collection of intelligence pursuant to ЬIection 702 of the Foreign Intelligence Surveillance Act // Office of the Director of National Intelligence. – URL: https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf (accessed: 30.05.2024).

37. Политика конфиденциальности WhatsApp // WhatsApp. – URL: https://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies (дата обращения: 30.05.2024).

38. Вехов: Facebook – инструмент информационной войны // Sputnik Молдова. – 2019. – 18 февраля. – URL: https://md.sputniknews.ru/20190218/vekhov-

facebook-instrument-informatsionnoy-voyny-24775421.html (дата обращения: 30.05.2024).

39. Мы можем закрыть Facebook уже завтра. Как России не проиграть в информационной войне? / Михаил Делягин. – URL: https://delyagin.ru/articles/192-deljagina-tsitirujut/90483-my-mozhem-zakryt-fa-ebook-uzhe-zavtra-kak-rossii-ne-proigrat-v-informatsionnoy-voyne (дата обращения: 14.03.2024).

40. *Holmes A.* 533 million Facebook users' phone numbers and personal data have been leaked online // Business Insider. – 2021. – April 3. – URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?utm_source=notification&utm_medium=referral (accessed: 30.05.2024).

41. Press release: Thousands expected to sue Facebook in mass action against privacy breach // Digital Rights Ireland. – 2021. – April 16. – URL: https://www.digitalrights.ie/facebook-breach/ (accessed: 30.05.2024).

42. DRI Facebook action // Digital Rights Ireland. – URL: https://www.digitalrights.ie/facebook/ (accessed: 30.05.2024).

43. *Wakefield J.* Coronavirus: Zoom is in everyone's living room – how safe is it? // BBC. – 2020. – 27 March. – URL: https://www.bbc.com/news/technology-52033217 (accessed: 14.03.2024).

44. *Marczak B., Scott-Railton J.* Move fast and roll your own crypto. A quick look at the confidentiality of zoom meetings // Citizen Lab. – 2020. – April 3. – URL: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ (accessed: 30.05.2024).

45. FORM S-1. Zoom Video Communications, Inc. March 22, 2019 // The United States Securities and Exchange Commission. – URL: https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm (accessed: 30.05.2024).

46. Zoom Video Communications US SEC Form 10-K (2020, 31 January) // Internet Archive. – URL: https://web.archive.org/web/20200511122414/https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa (accessed: 30.05.2024).

47. Zoom. Improving our policies as we continue to enable global collaboration. – URL: https://www.zoom.com/en/blog/improving-our-policies-as-we-continue-to-enable-global-collaboration/ (accessed: 30.05.2024).

48. Zoom access from China // University of California, Santa Barbara. – URL: https://help.lsit.ucsb.edu/hc/en-us/articles/360042172231-Zoom-Access-from-China (accessed: 14.03.2024).

49. "China support, my China colleagues cannot enter zoom meeting, why?" // Zoom Community. – URL: https://community.zoom.com/t5/Meetings/China-support-my-china-colleagues-cannot-enter-zoom-meeting-why/m-p/139630 (accessed: 30.05.2024).

50. Chinese regulator launches probe into Tencent, Weibo and Baidu // Bloomberg. – 2017. – 11 August. – URL: https://www.bloomberg.com/news/articles/2017-08-11/chinese-regulator-starts-probe-into-tencent-weibo-and-baidu (accessed: 30.05.2024).

51. 腾讯微信、新浪微博、百度贴吧涉嫌违反《网络安全法》被立案调查 // 中央网络安全和信息化委员会办公室 中华. – URL: http://www.cac.gov.cn/2017-08/11/c_1121467425.htm (accessed: 30.05.2024).

52. 公安机关互联网安全监督检查规定（公安部令第151号） // 中华人民共和国公安部 版权所有. – URL: https://www.mps.gov.cn/n6557558/c6263180/content.html (проверено 14.03.2024 г.).

53. *Жукова К.* Все «дыры» Zoom: чем рискуют пользователи самого популярного сервиса видеоконференций эпохи карантина // Forbes. – 2020. – 23 апреля. – URL: https://www.forbes.ru/tehnologii/398629-vse-dyry-zoom-chem-riskuyut-polzovateli-samogo-populyarnogo-servisa (дата обращения: 30.05.2024).

54. Zoom. Заявление о конфиденциальности // Zoom Video Communications. – URL: https://explore.zoom.us/ru/privacy/ (дата обращения: 30.05.2024).

55. Kaspersky Team. Сквозное шифрование: что это и зачем оно нужно вам // Блог Касперского. – URL: https://www.kaspersky.ru/blog/what-is-end-to-end-encryption/29075/ (проверено 14.03.2024 г.).

56. Сквозное шифрование (E2EE) конференций // Zoom Поддержка. – URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408 (дата обращения: 30.05.2024).

57. *Rosenblatt K.* Army bans TikTok following guidance from the Pentagon // NBC News. – 2019. – December 31. – URL: https://www.nbcnews.com/tech/tech-news/u-s-army-bans-tiktok-following-guidance-pentagon-n1109001 (accessed: 30.05.2024).

58. *Makena K.* The Army is in hot water over TikTok recruiting activity // The Verge. – 2021. – December 15. – URL: https://www.theverge.com/2021/12/14/22834405/tiktok-army-marco-rubio-ban-report-government-personal-devices (accessed: 30.05.2024).

59. Regarding the acquisition of Musical.ly by ByteDance Ltd. A Presidential Document by the Executive Office of the President on 08/14/2020 //

U.S. Department of the Treasury. – URL: https://home.treasury.gov/system/files/136/EO-on-TikTok-8-14-20.pdf (accessed: 30.05.2024).

60. *Pettersson E., Glovin D., Brody B.* TikTok sues Trump to challenge U.S. Government restrictions // Bloomberg. – 2020. – 24 August. – URL: https://www.bloomberg.com/news/articles/2020-08-24/tiktok-says-it-s-suing-u-s-over-ban-claims-no-security-threat (accessed: 30.05.2024).

61. Why we are suing the Administration // TikTok. – 2020. – 24 August. – URL: https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit (accessed: 30.05.2024).

62. *Wells G., Tilley A.* Oracle wins bid for TikTok in U.S., beating Microsoft // The Wall Street Journal. – 2020. – September 14. – URL: https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-tiktoks-u-s-operations-11600039821 (accessed: 30.05.2024).

63. *Sherman A., Repko M.* TikTok likely to announce sale of U.S. operations in the coming days in $20 billion to $30 billion range // CNBC. – 2020. – 27 August. – URL: https://www.cnbc.com/2020/08/27/tiktok-likely-to-announce-sale-us-operations-in-the-coming-days.html (accessed: 30.05.2024).

64. Microsoft statement on TikTok // Official Microsoft Blog. – URL: https://blogs.microsoft.com/blog/2020/09/13/microsoft-statement-on-tiktok/ (accessed: 30.05.2024).

65. Executive Order 14034 of June 9, 2021. Protecting Americans' Sensitive Data from Foreign Adversaries // Federal Register. – URL: https://www.federalregister.gov/d/2021-12506 (accessed: 30.05.2024).

66. Executive Order 13873 of May 15, 2019. Securing the Information and Communications Technology and Services Supply Chain // Federal Register. – URL: https://www.federalregister.gov/d/2019-10538 (accessed: 30.05.2024).

67. Rubio, Gallagher introduce bipartisan legislation to ban TikTok // Senator Rubio. – URL: https://www.rubio.senate.gov/rubio-gallagher-introduce-bipartisan-legislation-to-ban-tiktok/ (accessed: 14.03.2024).

68. S.1143 – No TikTok on government devices Act // United States Congress. – URL: https://www.congress.gov/bill/117th-congress/senate-bill/1143 (accessed: 30.05.2024).

69. *Dilanian K., Shabad R.* The DOJ and FBI are investigating TikTok over allegations that employees spied on journalists // NBC. – 2023. – March 18. – URL: https://www.nbcnews.com/politics/justice-department/doj-fbi-are-investigating-tiktok-allegations-employees-spied-journalis-rcna75497 (accessed: 30.05.2024).

70. S.686 – Restrict Act // United States Congress. – URL: https://www.congress.gov/bill/118th-congress/senate-bill/686 (accessed: 30.05.2024).

71. H.R.7521 – Protecting Americans from Foreign Adversary Controlled Applications Act // United States Congress. – URL: https://www.congress.gov/bill/118th-congress/house-bill/7521 (accessed: 30.05.2024).

72. *Huang R.* China signals opposition to forced sale of TikTok in the U.S. // The Wall Street Journal. – 2024. – March 15. – URL: https://www.wsj.com/tech/tiktok-ban-chinese-owners-bytedance-1a857a06 (accessed: 30.05.2024).

Петрунин Юрий Юрьевич, доктор философских наук, профессор, заведующий кафедрой «Математические методы и информационные технологии в управлении» факультета государственного управления Московского государственного университета имени М.В. Ломоносова, руководитель секции «Управление знаниями» Научного совета РАН по методологии искусственного интеллекта, руководитель Центра анализа больших данных в общественных науках. Область научных интересов: искусственный интеллект, нейрокомпьютинг, анализ данных, наукометрия. Имеет более 150 публикаций. E-mail: petrunin@spa.msu.ru

Бухарин Владислав Викторович, кандидат исторических наук, доцент кафедры «Математические методы и информационные технологии в управлении» факультета государственного управления Московского государственного университета имени М.В. Ломоносова. Область научных интересов: информационная безопасность, национальная безопасность, международные отношения, геополитика, история Великобритании. E-mail: bukharin@spa.msu.ru

DOI: 10.17212/2782-2230-2024-2-25-54

From information security to national security: the confrontation between us and chinese IT-companies*

Yu.Yu. Petrunin[1], V.V. Bukharin[2]

[1] *Lomonosov Moscow State University, 27/4 Lomonosov Prospekt, Moscow, 119991, Russian Federation, DSc (Philosophical Sciences), professor, head of the mathematical methods and information technology in management department. E-mail: petrunin@spa.msu.ru*
[2] *Lomonosov Moscow State University, 27/4 Lomonosov Prospekt, Moscow, 119991, Russian Federation, Ph.D. (Historical Sciences), associate professor of the mathematical methods and information technology in management department. E-mail: bukharin@spa.msu.ru*

The article examines certain aspects of the activities of large IT-companies that are closely related to the problem of information security, ensuring digital sovereignty as the basis of national security. Special attention is paid to the struggle of transnational IT-corporations of the USA and China for alternative markets, as well as a number of restrictions imposed on them by the laws of foreign countries. Based on a study of official documents of American and Chinese government agencies and IT-corporations, as well as media materials, the authors conclude that the geopolitical interests of the United States and China are in contact with the goals of big business and force governments to resort to various kinds of prohibitions and protectionist measures. IT-corporations in the USA and China, developers of messengers and social networks do not pay enough attention to the information security of their users.

Keywords: information security, IT-corporations, national security, information warfare, digital sovereignty, Microsoft, Google, ByteDance, TikTok, WeChat, WhatsApp, Zoom, cybersecurity

REFERENCES

1. Bukharin V.V. Komponenty tsifrovogo suvereniteta Rossiiskoi Federatsii kak tekhnicheskaya osnova informatsionnoi bezopasnosti [The Russian's digital sovereignty as a technical basis of information security]. *Vestnik MGIMO-Universiteta = MGIMO Review of International Relations*, 2016, no. 6 (51), pp. 76–91. DOI: 10.24833/2071-8160-2016-6-51-76-91.

2. Moore G.J. Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies. *Journal of Chinese Political Science*, 2023, vol. 28 (1), pp. 151–167. DOI: 10.1007/s11366-022-09814-2.

3. Tsvetkova N., Sytnik A. Tsifrovoe protivostoyanie SShA i KNR: ekonomicheskoe i politicheskoe izmereniya [Digital confrontation between USA and China:

* *Received 16 May 2024.*

economic and political dimensions]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya = World Economy and International Relations*, 2023, vol. 67, no. 11, pp. 15–23. DOI: 10.20542/0131-2227-2023-67-11-15-23.

4. Gamza L.A. Tekhnologicheskoe protivostoyanie SShA i Kitaya v Evrope [Technological confrontation between USA and China in Europe]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya = World Economy and International Relations*, 2023, vol. 65, no. 7, pp. 98–105. DOI: 10.20542/0131-2227-2021-65-7-98-105.

5. Katkova E.Yu., Yunyushkina A.S. Kitaiskie kontseptsii i vozmozhnosti v informatsionnoi voine: sopernichestvo KNR i SShA v kiberprostranstve [Chinese strategies and opportunities in information warfare: China–US rivalry in cyberspace]. *Vestnik RUDN. Seriya: Vseobshchaya istoriya = RUDN Journal of World History*, 2022, vol. 14 (2), pp. 197–210. DOI: 10.22363/2312-8127-2022-14-2-197-210.

6. Julian N. United States' and China's cybersecurity policies: collaboration or confrontation? *The Sigma Iota Rho (SIR) Journal of International Relations*, 2021, January 24. Available at: https://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation (accessed 29.05.2024).

7. Bukharin V.V. [BRICS cybersecurity]. *Gosudarstvennoe upravlenie Rossiiskoi Federatsii: povestka dnya vlasti i obshchestva* [Public administration of the Russian Federation: the agenda of government and society]. Proceedings of the XVI International Conference (May 31 – June 02, 2018). Moscow, 2019, pp. 552–559. (In Russian).

8. Cheung T.M. The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, 2018, vol. 3 (3), pp. 306–326. DOI: 10.1080/23738871.2018.1556720.

9. Kurylev K.P., Parkhitko N.P., Smolik N.G. Natsional'nye rezhimy regulirovaniya seti internet v stranakh SNG [National internet regulatory regimes in the CIS countries]. *Postsovetskie issledovaniya = Journal Post-Soviet Studies*, 2021, vol. 4 (8), pp. 705–718. DOI: 10.24412/2618-7426-2021-8-705-718.

10. Endeley R.E. End-to-end encryption in messaging services and national security – case of Whatsapp messenger. *Journal of Information Security*, 2018, vol. 9 (1), pp. 95–99. DOI: 10.4236/jis.2018.91008.

11. Video social networking app Musical.ly agrees to settle FTC allegations that it violated children's privacy law. *Federal Trade Commission*, 2019, February 27. Available at: https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc (accessed 29.05.2024).

12. Zhaoyin F., Cheetham J. Trump WeChat ban 'an unwelcome signal' for Chinese community. *BBC*, 2020, August 10. Available at: https://www.bbc.com/news/world-asia-china-53686507 (accessed 09.01.2024).

13. Shen X. The story of China's Great Firewall, the world's most sophisticated censorship system. *South China Morning Post*, 2019, November 7. Available at: https://www.scmp.com/abacus/who-what/what/article/3089836/story-chinas-great-firewall-worlds-most-sophisticated (accessed 29.05.2024).

14. Mills E. Google to censor China Web searches. *CNET*, 2006, January 25. Available at: https://www.cnet.com/news/google-to-censor-china-web-searches/ (accessed 29.05.2024).

15. Watts J. Microsoft helps China to censor bloggers. *The Guardian*, 2005, June 15. Available at: https://www.theguardian.com/technology/2005/jun/15/newmedia.microsoft (accessed 29.05.2024).

16. Kristof N. Microsoft and Chinese Censorship. *The New York Times*, 2009, June 24. Available at: https://archive.nytimes.com/kristof.blogs.nytimes.com/2009/06/24/microsoft-and-chinese-censorship/?searchResultPosition=6 (accessed 29.05.2024).

17. Informatsiya po delu № 02-2473/2022 [Information on case No. 02-2473/2022]. *Ofitsial'nyi portal sudov obshchei yurisdiktsii g. Moskvy* [The official website of the Courts of general jurisdiction of Moscow]. Available at: https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35?participants=meta (accessed 29.05.2024).

18. 80 pct of netizens agree China should punish Facebook. *People's Daily Online*, 2009, July 10. Available at: https://en.people.cn/90001/90776/90882/6697993.html (accessed 01.08.2020).

19. Kotsar Yu., Bevza D. Protesty lishili Kitai Instagram [Protests deprived China of Instagram]. *Газета.Ru*, 2014, 29 September. (In Russian). Available at: https://www.gazeta.ru/tech/2014/09/29_a_6240045.shtml (accessed 29.05.2024).

20. Isaac M. Facebook said to create censorship tool to get back into China. *The New York Times*, 2016, November 22. Available at: https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html (accessed 29.05.2024).

21. Counter-Terrorism Law (as amended in 2018). *China Law Translate*. Available at: https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/ (accessed 29.05.2024).

22. Creemers R., Webster G., Triolo P. *Translation: Cybersecurity Law of the People's Republic of China* (Effective June 1, 2017). Stanford Cyber Policy Center. Available at: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (accessed 29.05.2024).

23. Abkowitz A., Seetharaman D., Dou E. Facebook is trying everything to re-enter China – and it's not working. *The Wall Street Journal*, 2017, January 30.

Available at: https://www.wsj.com/articles/mark-zuckerbergs-beijing-blues-1485791106 (accessed 29.05.2024).

24. Economy E.C. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*, 2018, June 29. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown (accessed 29.05.2024).

25. Ye J. China tightens Great Firewall by declaring unauthorised VPN services illegal. *South China Morning Post*, 2017, January 23. Available at: https://www.scmp.com/news/china/policies-politics/article/2064587/chinas-move-clean-vpns-and-strengthen-great-firewall (accessed 29.05.2024).

26. ChinaPower. *How Web-connected is China?* Available at: https://chinapower.csis.org/web-connectedness/ (accessed 29.05.2024).

27. China's internet underground fights for its life. *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2018-03-01/china-s-internet-underground-fights-for-its-life (accessed 29.05.2024).

28. Bradsher K. China blocks WhatsApp, broadening online censorship. *The New York Times*, 2017, September 25. Available at: https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html (accessed 29.05.2024).

29. Mozur P. China disrupts WhatsApp service in online clampdown. *The New York Times*, 2017, July 18. Available at: https://www.nytimes.com/2017/07/18/technology/whatsapp-facebook-china-internet.html (accessed 29.05.2024).

30. WhatsApp design feature means some encrypted messages could be read by third party. *The Guardian*, 2017, January 13. Available at: https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages (accessed 29.05.2024).

31. Whittaker Z. US says it doesn't need secret court's approval to ask for encryption backdoors. *ZDNet*, 2017, December 7. Available at: https://www.zdnet.com/article/us-says-it-does-not-need-courts-to-approve-encryption-backdoors/ (accessed 29.05.2024).

32. FISA questions (July 2017). Wyden's encryption backdoor question. *Web archive*. Available at: https://web.archive.org/web/20230106172742/https://www.documentcloud.org/documents/4320971-FISA-questions-July-2017.html (accessed 29.05.2024).

33. Gellman B., Lindeman T. Inner workings of a top-secret spy program. *Washington Post*, 2013, June 29. Available at: https://web.archive.org/web/20170830105407/https://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/ (accessed 29.05.2024).

34. Greenwald G., MacAskill E., Poitras L., Ackerman S., Rushe D. Microsoft handed the NSA access to encrypted messages. *The Guardian*, 2013, July 12.

Available at: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (accessed 29.05.2024).

35. Microsoft. *About our practices and your data*. Available at: https://blogs.microsoft.com/datalaw/our-practices/#did-participate-in-prism-program (accessed 29.05.2024).

36. Facts on the collection of intelligence pursuant to Section 702 of the Foreign Intelligence Surveillance Act. *Office of the Director of National Intelligence*. Available at: https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf (accessed 30.05.2024).

37. WhatsApp Privacy Policy. *WhatsApp*. Available at: https://www.whatsapp.com/legal/updates/privacy-policy?eea=0#privacy-policy-updates-how-we-work-with-other-facebook-companies (accessed 30.05.2024).

38. Vekhov: Facebook – instrument informatsionnoi voiny [Vekhov: Facebook is an information warfare tool]. *Sputnik Moldova*, 2019, 18 February. (In Russian). Available at: https://md.sputniknews.ru/20190218/vekhov-facebook-instrument-informatsionnoy-voyny-24775421.html (accessed 30.05.2024).

39. Delyagin Mikhail. *My mozhem zakryt' Facebook uzhe zavtra. Kak Rossii ne proigrat' v informatsionnoi voine?* [We can close Facebook tomorrow. How can Russia not lose in the information war?]. (In Russian). Available at: https://delyagin.ru/articles/192-deljagina-tsitirujut/90483-my-mozhem-zakryt-facebook-uzhe-zavtra-kak-rossii-ne-proigrat-v-informatsionnoy-voyne (accessed 14.03.2024).

40. Holmes A. 533 million Facebook users' phone numbers and personal data have been leaked online. *Business Insider*, 2021, April 3. Available at: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?utm_source=notification&utm_medium=referral (accessed 30.05.2024).

41. Press release: Thousands expected to sue Facebook in mass action against privacy breach. *Digital Rights Ireland*, 2021, April 16. Available at: https://www.digitalrights.ie/facebook-breach/ (accessed 30.05.2024).

42. DRI Facebook action. *Digital Rights Ireland*. Available at: https://www.digitalrights.ie/facebook/ (accessed 30.05.2024).

43. Wakefield J. Coronavirus: Zoom is in everyone's living room – how safe is it? *BBC*, 2020, 27 March. Available at: https://www.bbc.com/news/technology-52033217 (accessed 14.03.2024).

44. Marczak B., Scott-Railton J. Move fast and roll your own crypto. A quick look at the confidentiality of zoom meetings. *Citizen Lab*, 2020, April 3. Available at: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ (accessed 30.05.2024).

45. FORM S-1. Zoom Video Communications, Inc. March 22, 2019. *The United States Securities and Exchange Commission*. Available at: https://www.sec.gov/Archives/edgar/data/1585521/000119312519083351/d642624ds1.htm (accessed 30.05.2024).

46. Zoom Video Communications US SEC Form 10-K (2020, 31 January). *Internet Archive*. Available at: https://web.archive.org/web/20200511122414/https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa (accessed 30.05.2024).

47. Zoom. *Improving our policies as we continue to enable global collaboration*. Available at: https://www.zoom.com/en/blog/improving-our-policies-as-we-continue-to-enable-global-collaboration/ (accessed 30.05.2024).

48. Zoom access from China. *University of California, Santa Barbara*. Available at: https://help.lsit.ucsb.edu/hc/en-us/articles/360042172231-Zoom-Access-from-China (accessed 14.03.2024).

49. "China support, my China colleagues cannot enter zoom meeting, why?". *Zoom Community*. Available at: https://community.zoom.com/t5/Meetings/China-support-my-china-colleagues-cannot-enter-zoom-meeting-why/m-p/139630 (accessed 30.05.2024).

50. Chinese regulator launches probe into Tencent, Weibo and Baidu. *Bloomberg*, 2017, 11 August. Available at: https://www.bloomberg.com/news/articles/2017-08-11/chinese-regulator-starts-probe-into-tencent-weibo-and-baidu (accessed 30.05.2024).

51. Tencent WeChat, Sina Weibo and Baidu Post Bars were investigated for suspected violations of the "Network Security Act." *Office of the Central Commission for Network Security and Information Technology of China*. (In Chinese). Available at: http://www.cac.gov.cn/2017-08/11/c_1121467425.htm (accessed 30.05.2024).

52. Regulation on the Supervision and Verification of Internet Security by Public Security Authorities (Order No. 151 of the Ministry of Public Security). *Ministry of Public Security of the People's Republic of China*. (In Chinese). Available at: https://www.mps.gov.cn/n6557558/c6263180/content.html (accessed 30.05.2024).

53. Zhukova K. Vse «dyry» Zoom: chem riskuyut pol'zovateli samogo populyarnogo servisa videokonferentsii epokhi karantina [All vulnerability of Zoom: what are the risks of users of the most popular video conferencing service of the quarantine era]. *Forbes*, 2020, 23 April. (In Russian). Available at: https://www.forbes.ru/tehnologii/398629-vse-dyry-zoom-chem-riskuyut-polzovateli-samogo-populyarnogo-servisa (accessed 30.05.2024).

54. Zoom. Zayavlenie o konfidentsial'nosti [Zoom Privacy Statement]. *Zoom Video Communications*. Available at: https://explore.zoom.us/ru/privacy/ (accessed 30.05.2024).

55. Kaspersky Team. Skvoznoe shifrovanie: chto eto i zachem ono nuzhno vam [Kaspersky Team. End-to-end encryption: what is it and why do you need it]. *Blog Kasperskogo* [Kaspersky's blog]. Available at: https://www.kaspersky.ru/blog/what-is-end-to-end-encryption/29075/ (accessed 30.05.2024).

56. Skvoznoe shifrovanie (E2EE) konferentsii [End-to-end encryption (E2EE) of conferences]. *Zoom Podderzhka* [Zoom Support]. Available at: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408 (accessed 30.05.2024).

57. Rosenblatt K. Army bans TikTok following guidance from the Pentagon. *NBC News*, 2019, December 31. Available at: https://www.nbcnews.com/tech/tech-news/u-s-army-bans-tiktok-following-guidance-pentagon-n1109001 (accessed 30.05.2024).

58. Makena K. The Army is in hot water over TikTok recruiting activity. *The Verge*, 2021, December 15. Available at: https://www.theverge.com/2021/12/14/22834405/tiktok-army-marco-rubio-ban-report-government-personal-devices (accessed 30.05.2024).

59. Regarding the Acquisition of Musical.ly by ByteDance Ltd. A Presidential Document by the Executive Office of the President on 08/14/2020. *U.S. Department of the Treasury*. Available at: https://home.treasury.gov/system/files/136/EO-on-TikTok-8-14-20.pdf (accessed 30.05.2024).

60. Pettersson E., Glovin D., Brody B. TikTok Sues Trump to Challenge U.S. Government Restrictions. *Bloomberg*, 2020, 24 August. Available at: https://www.bloomberg.com/news/articles/2020-08-24/tiktok-says-it-s-suing-u-s-over-ban-claims-no-security-threat (accessed 30.05.2024).

61. Why we are suing the Administration. *TikTok*, 2020, 24 August. Available at: https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit (accessed 30.05.2024).

62. Wells G., Tilley A. Oracle wins bid for TikTok in U.S., beating Microsoft. *The Wall Street Journal*, 2020, September 14. Available at: https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-tiktoks-u-s-operations-11600039821 (accessed 30.05.2024).

63. Sherman A., Repko M. TikTok likely to announce sale of U.S. operations in the coming days in $20 billion to $30 billion range. *CNBC*, 2020, 27 August. Available at: https://www.cnbc.com/2020/08/27/tiktok-likely-to-announce-sale-us-operations-in-the-coming-days.html (accessed 30.05.2024).

64. Microsoft statement on TikTok. *Official Microsoft Blog*. Available at: https://blogs.microsoft.com/blog/2020/09/13/microsoft-statement-on-tiktok/ (accessed 30.05.2024).

65. Executive Order 14034 of June 9, 2021. Protecting Americans' Sensitive Data from Foreign Adversaries. *Federal Register*. Available at: https://www.federalregister.gov/d/2021-12506 (accessed 30.05.2024).

66. Executive Order 13873 of May 15, 2019. Securing the Information and Communications Technology and Services Supply Chain. *Federal Register*. Available at: https://www.federalregister.gov/d/2019-10538 (accessed 30.05.2024).

67. Rubio, Gallagher introduce bipartisan legislation to ban TikTok. *Senator Rubio*. Available at: https://www.rubio.senate.gov/rubio-gallagher-introduce-bipartisan-legislation-to-ban-tiktok/ (accessed 14.03.2024).

68. S.1143 – No TikTok on government devices Act. *United States Congress*. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/1143 (accessed 30.05.2024).

69. Dilanian K., Shabad R. The DOJ and FBI are investigating TikTok over allegations that employees spied on journalists. *NBC*, 2023, March 18. Available at: https://www.nbcnews.com/politics/justice-department/doj-fbi-are-investigating-tiktok-allegations-employees-spied-journalis-rcna75497 (accessed 30.05.2024).

70. S.686 – Restrict Act. *United States Congress*. Available at: https://www.congress.gov/bill/118th-congress/senate-bill/686 (accessed 30.05.2024).

71. H.R.7521 – Protecting Americans from Foreign Adversary Controlled Applications Act. *United States Congress*. Available at: https://www.congress.gov/bill/118th-congress/house-bill/7521 (accessed 30.05.2024).

72. Huang R. China signals opposition to forced sale of TikTok in the U.S. *The Wall Street Journal*, 2024, March 15. Available at: https://www.wsj.com/tech/tiktok-ban-chinese-owners-bytedance-1a857a06 (accessed 30.05.2024).

Для цитирования:

Петрунин Ю.Ю., Бухарин В.В. От информационной безопасности к национальной: противоборство IT-компаний США и КНР // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 25–54. – DOI: 10.17212/2782-2230-2024-2-25-54.

For citation:

Petrunin Yu.Yu., Bukharin V.V. Ot informatsionnoi bezopasnosti k natsional'noi: protivoborstvo IT kompanii SShA i KNR [From information security to national security: the confrontation between US and Chinese IT-companies]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 25–54. DOI: 10.17212/2782-2230-2024-2-25-54.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 55–68

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-55-68

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ*

Н.Е. КАРПОВА[1], А.А. БАБИНОВА[2]

[1] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность». E-mail: esib@samgtu.ru*
[2] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, ассистент кафедры «Прикладная математика и информатика». E-mail: anyuta.babinova2000@yandex.ru*

При современном развитии информационных технологий, ресурсов и компьютеризации общества во всём мире в каждой из сфер деятельности человека не обходится без информационных технологий. Некоторые из них уникальны и приносят доход своей уникальностью, и вследствие этого одной из наиболее более актуальных становится проблема обеспечения информационной безопасности в любых организациях и предприятиях, для любой сферы и бизнес-деятельности. Люди в связи со стремлением получить выгоду могут совершать преступные действия по отношению к источникам доходов, коими всегда является информация. Самым распространенным таким источником являются персональные данные. В любой организации и на любых предприятиях существуют угрозы безопасности информации, которая содержит персональные данные. Эта информация может быть утрачена, скопирована, изменена или заблокирована как злоумышленником из корыстных побуждений, так и допущенным персоналом по ошибке и неосторожности. Потеря конфиденциальной информации может повлечь как незначительный ущерб, так и весьма серьезные последствия. Поэтому важную роль в сохранении и улучшении деятельности организаций играет обеспечение безопасности персональных данных, так как эта проблема существует во всех сферах жизнедеятельности.

В настоящей статье рассмотрены вопросы, связанные с разработкой системы по обеспечению безопасности персональных данных в информационной системе предприятия. Во время выполнения работы были проанализированы нормативно-правовые акты в сфере защиты и обработки персональных данных в информационной системе предприятия, был осуществлен анализ существующих средств защиты и исходной защищенности ИСПДн.

* Статья получена 20 апреля 2024 г.

В результате выполнения работы была разработана система защиты персональных данных в ИСПДн. Был произведен выбор технических и организационных мер, а также обоснование оборудования для системы защиты.

Ключевые слова: персональные данные, конфиденциальная информация, информационная система персональных данных, информационные технологии, исходная защищенность, актуальные угрозы, нарушитель, меры по обеспечению безопасности, система защиты

ВВЕДЕНИЕ

В современном мире, где информационные технологии, ресурсы и компьютеризация общества играют ключевую роль, использование информационных технологий становится неотъемлемой частью всех сфер деятельности. Некоторые из этих технологий уникальны и приносят доход за счет своей уникальности. В связи с этим проблема обеспечения информационной безопасности в организациях и предприятиях, независимо от их сферы деятельности, становится одной из самых актуальных.

Из-за стремления людей к личной выгоде возникают ситуации, когда они совершают преступные действия в отношении источников дохода, которыми часто является информация. Одним из самых распространенных таких источников являются персональные данные. В любой организации и на любом предприятии существуют угрозы безопасности информации, содержащей персональные данные. Эта информация может быть потеряна, скопирована, изменена или заблокирована как злоумышленником из корыстных побуждений, так и по ошибке или неосторожности со стороны персонала. Потеря конфиденциальной информации может привести как к незначительным убыткам, так и к серьезным последствиям. Поэтому обеспечение безопасности персональных данных играет важную роль в сохранении и улучшении деятельности организаций, поскольку эта проблема актуальна во всех сферах жизнедеятельности.

Персональные данные обладают конкретной стоимостной ценностью, которая определяется как потенциальной прибылью от их использования, так и возможным ущербом от несанкционированного доступа. Затраты на обеспечение защиты таких данных постоянно растут, но компании стремятся избегать лишних расходов, предпочитая приобретать только необходимые решения для построения надежной системы защиты информации. Однако для оптимального выбора таких средств защиты необходима оценка их эффективности и соответствия требованиям конкретной ситуации, включая функциональные особенности и экономическую целесообразность.

Следует отметить, что обеспечение безопасности персональных данных в информационной системе предприятия требует не только обучения персонала, организации охраны объектов и других организационных мер по защите информации, но и выявления и изучения возможных каналов утечки данных, определения актуальных угроз, а также использования специализированных технических средств, способных противодействовать различным видам атак злоумышленников.

ИССЛЕДОВАНИЕ

Защита персональных данных регулируется Федеральным законом РФ от 27.07.2006 № 152 «О персональных данных». Он определяет основные термины и принципы обработки персональных данных физических и юридических лиц, а также предписывает требования по организации работы с такими данными для операторов и их ответственность в случае нарушения законодательства.

Для выполнения требований Закона «О персональных данных» было принято постановление Правительства Российской Федерации от 01.11.2012 № 1119 [3]. В пункте 4 этого документа установлено правило относительно выбора средств защиты персональных данных, согласно которому выбор таких средств должен соответствовать нормативным актам Федеральной службы по техническому и экспортному контролю (ФСТЭК) России.

Кроме этого, в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ [4] установление требований по защите ПД и контроль за их исполнением отнесен к компетенции ФСТЭК России.

В целях исполнения Закона «О персональных данных» [2] и постановления Правительства Российской Федерации от 01.11.2012 № 1119 [3] издан приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 [5], конкретизирующий состав и содержимое мер по обеспечению сохранности персональных данных.

Для оценки угроз информационной безопасности используется методика, утвержденная 5 февраля 2021 года Федеральной службой по техническому и экспортному контролю под названием «Методика оценки угроз безопасности информации» [7]. Этот документ опирается на классический подход к анализу угроз, который включает в себя идентификацию потенциальных рисков негативных последствий от угроз информационной безопасности, выявление источников этих угроз, оценку их возможностей и разработку сцена-

риев их реализации. Анализ проводится последовательно: определение рисков, выявление нарушителей, анализ их тактик и методов (разработка сценариев) и затем принятие решения о степени актуальности угрозы на основе этих данных.

В статье Гаврющенко А.П. «О методике определения актуальных угроз информационной безопасности с использованием БДУ ФСТЭК» рассмотрена методика оценки угроз безопасности, определены этапы определения актуальных угроз информационной безопасности, сопровождающиеся практическими примерами [9].

В качестве объекта исследования был выбран кабинет бухгалтерии АО «АИМ», имеющий площадь 40 квадратных метров и оснащеннный автоматизированными рабочими местами (АРМ). В нем установлены окна из ПВХ, а входная дверь выполнена из дерева.

Документы, обрабатываемые в ИСПДн, относятся к категории «иные персональные данные». Для обеспечения безопасности в системе бухгалтерии применяется антивирусное программное обеспечение Kaspersky Endpoint Security 11 и разграничение доступом в соответствии с политикой безопасности. Для обработки данных в ИСПДн используется программный комплекс 1С: Предприятие и 1С: Зарплата и управление персоналом. Также используется одно из клиентских приложений системы 1С: Предприятие – тонкий клиент.

После определения средств защиты ПДн в ИСПДн «Бухгалтерия» был определен уровень исходной защищенности согласно п. 2 «Методики» [8] ФСТЭК. Уровень исходной защищенности средний, так как не менее 70 % характеристик ИСПДн соответствуют уровню не ниже среднего.

Затем с помощью пункта 5.1.3 «Методики оценки угроз безопасности информации» [7] был составлен перечень актуальных нарушителей, среди них:

– персонал, поддерживающий работоспособность систем и сетей (администраторы, охранники, уборщики и прочие) (внутренний нарушитель);

– сотрудники, имеющие разрешение на использование систем и сетей (внутренний нарушитель).

После определения актуальных нарушителей следует определить уровни возможностей нарушителей, которые могут реализовывать угрозы безопасности информации. Уровни возможностей будем определять в соответствии с приложениями 8 и 9 к «Методике оценки угроз безопасности информации» [7]. Для этого были сопоставлены данные из указанного выше документа с перечнем актуальных нарушителей. Результаты сопоставления приведены в таблице.

Уровни возможностей актуальных нарушителей

№ п/п	Виды ущерба	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1: нарушение конфиденциальности персональных данных граждан	Персонал, поддерживающий работоспособность систем и сетей (администраторы, охранники, уборщики и прочие)	Внутренний	Н2
2		Сотрудники, имеющие разрешение на использование систем и сетей	Внутренний	Н1

Основным объектом атак является программное обеспечение 1С, поскольку оно служит для выполнения большинства задач пользователей.

Проанализируем неблагоприятные последствия, которые могут возникнуть в результате несанкционированного доступа к ресурсам 1С:

– раскрытие личных данных сотрудников, включая их адреса и контактную информацию, может привести к нежелательному вмешательству в их частную жизнь;

– несанкционированное изменение личных данных сотрудников может привести к внесению неверной информации в официальные документы, такие как приказы, распоряжения, заявления и т. д.;

– несанкционированное изменение информации о заработной плате и премиях сотрудников может привести к юридическим и финансовым убыткам, неправильному определению размера выплат.

Затем проводим анализ угроз. В ходе исследования были выявлены следующие актуальные угрозы.

1. Запуск специально разработанных программ, реализующих НСД к ИСПДн. Эти угрозы направлены на выполнение таких действий, как уничтожение, копирование, перемещение, форматирование носителей информации и т. д. Это происходит с использованием стандартных функций операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для этого программных средств, таких как вирус-шифровальщик (троянский конь).

2. Подбор паролей. Злоумышленник может осуществить атаку, применяя различные методы, включая простой перебор, использование специальных словарей или внедрение вредоносного программного обеспечения для перехвата пароля. В случае успеха злоумышленник может установить «заднюю дверь» для последующего доступа. Для смягчения такой угрозы можно увеличить временную сложность процесса подбора пароля, например, увеличив его длину и сложность или ограничив количество неверных попыток ввода пароля за определенный промежуток времени. Эти меры могут быть реализованы через сочетание организационных и технических действий.

3. Нарушения безопасности персональных данных, вызванные ошибками пользователей. Из-за человеческого фактора злоумышленник может добраться до данных. Пользователи могут хранить пароли на бумаге, оставлять их рядом с компьютером или передавать третьим лицам. Кроме того, непреднамеренные действия пользователей могут нарушить целостность, доступность и конфиденциальность персональных данных.

Выше были перечислены актуальные угрозы ПДн для рассматриваемой системы, определены потенциальные нарушители. Перечень актуальных угроз составлен экспертным методом в соответствии с Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн [8].

Таким образом, после оценки эффективности текущих защитных механизмов мы пришли к выводу, что требуется усиление системы защиты путем внедрения дополнительных мер, так как выявлены актуальные угрозы.

Исходя из перечня актуальных угроз, сформированы требования к комплексу мер по защите ПДн.

Первое требование – устранить запуск специально разработанных программ, реализующих НСД к ИСПДн; второе – предотвратить выявление паролей; третье – сократить ошибочные действия пользователей, приводящие к нарушению безопасности персональных данных.

В ходе защиты ИСПДн «Бухгалтерия» следует выбрать средства защиты информации, которые покрывают своими функциональными возможностями весь комплекс предъявляемых мер. Ниже приведена структура комплекса мер защиты (рис. 1 и 2).

Следуя этим требованиям, были выбраны технические средства защиты и разработаны организационные меры, которые полностью удовлетворяют всем требованиям. Мы отдали предпочтение сертифицированным средствам защиты, и в качестве технического решения была выбрана платформа SecretNetStudio.

Рис. 1. Комплекс мер защиты

Рис. 2. Структура комплекса мер защиты ПДн в ИСПДн «Бухгалтерия»

Организационно-распорядительная документация – это набор неотъемлемых документов, который определяет роли, обязанности, цели и права всех работников, включая руководителя и администратора безопасности, в рамках информационной системы по защите персональных данных.

В качестве организационной меры был проведен анализ уже имеющейся политики безопасности ИСПДн «Бухгалтерия», а также ее проверка на соответствие требованиям законодательства Российской Федерации в сфере защиты информации.

Поскольку часть документов политики безопасности не была актуализирована на момент проведения проверки (требовали модернизации и дополнения), было принято решение о внесении изменений в политику обработки и обеспечения безопасности персональных данных в информационной системе «Бухгалтерия», а также в документ, регламентирующий процессы обработки и обеспечения безопасности персональных данных в этой системе, чтобы они полностью соответствовали всем требованиям действующего законодательства Российской Федерации.

Было разработано приложение для сотрудников под названием Security Policy. Основная его цель – упростить процесс знакомства и подписания созданных документов, обеспечивающих безопасность информационной системы по защите персональных данных «Бухгалтерия». После того как пользователь из бухгалтерии вводит свои ФИО, возраст и должность, приложение предоставляет ему перечень необходимых документов. После ознакомления пользователь нажимает кнопку «согласен». Приложение записывает это действие в базу данных, включая ФИО пользователя и информацию о том, ознакомился он с документацией или нет.

Затем проводим повторный анализ угроз по «Методике определения актуальных угроз безопасности» [8]. Результаты повторного анализа приведены на рис. 3, на котором мы можем увидеть, что количество актуальных угроз снизилось до нуля, так как ни одна из угроз не имеет характеристик «возможность реализации» и «опасность» одновременно на втором уровне.

Исходя из повторного анализа угроз, можно сделать вывод, что после внедрения и реализации комплекса мер защиты персональных данных в информационную систему «Бухгалтерия» АО «АИМ» вероятность реализации актуальных угроз стала «низкой». Это означает, что и угрозы перешли в разряд «неактуальных».

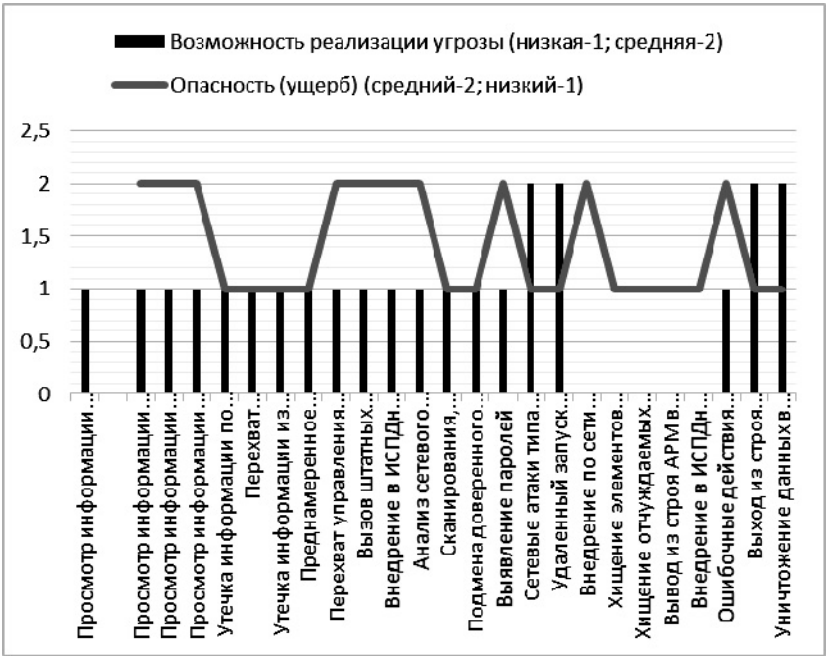


Рис. 3. Повторный анализ угроз

ЗАКЛЮЧЕНИЕ

Таким образом, был проведен анализ нормативно-правовых актов в сфере обработки персональных данных и требований к их защите, оценен исходный уровень безопасности информационной системы персональных данных и имеющихся средств защиты, а также проанализированы существующие актуальные угрозы. На основе этого анализа были выбраны организационные и технические меры защиты информационной системы.

Была выполнена установка и настройка Secret Net Studio. В ходе этой работы произведена актуализация политики безопасности и ее приложений. Дополнительно было разработано клиентское приложение Security Policy.

В результате была успешно выполнена задача по созданию системы защиты для обеспечения безопасности персональных данных в информационной системе предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 30.05.2024).

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 30.05.2024).

3. Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон "О персональных данных"» // КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_117437/ (дата обращения: 30.05.2024).

4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.05.2024).

5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 30.05.2024).

6. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Гарант.Ру: сайт. – URL: https://base.garant.ru/193875 (дата обращения: 30.05.2024).

7. Методический документ ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации» // ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 30.05.2024).

8. Методический документ ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // ФСТЭК России – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (дата обращения: 30.05.2024).

9. *Гаврющенко А.П.*, *Масленников А.В.* О методике определения актуальных угроз информационной безопасности с использованием БДУ ФСТЭК // Auditorium. – 2022. – № 2 (34). – С. 37–43.

10. Государственный реестр сертифицированных средств защиты информации // ФСТЭК России – URL: https://reestr.fstec.ru/reg3 (дата обращения: 30.05.2024).

11. Secret Net Studio 8.5. Руководство администратора. Настройка и эксплуатация. – М.: Код безопасности, 2019. – 106 с.

12. Secret Net Studio 8.5. Руководство администратора. Локальная защита. – М.: Код безопасности, 2019. – 159 с.

13. *Исаев А.С., Хлюпина Е.А.* Правовые основы организации защиты персональных данных. – СПб.: НИУ ИТМО, 2014. – 106 с. – URL: https://books.ifmo.ru/file/pdf/1570.pdf (дата обращения: 30.05.2024).

14. *Слепов О.* Защита персональных данных. – URL: https://www.jetinfo.ru/zaschita-personalnykh/ (дата обращения: 30.05.2024).

15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка): (утв. ФСТЭК РФ 15.02.2008) // КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_99662 (дата обращения: 30.05.2024).

Карпова Надежда Евгеньевна, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Основные направления научных исследований – автоматизированные интеллектуальные системы и автоматизированные информационно-измерительные системы. Имеет более 100 публикаций. E-mail: esib@samgtu.ru

Бабинова Анна Андреевна, ассистент кафедры «Информатика и прикладная математика» Самарского государственного технического университета. E-mail: anyuta.babinova2000@yandex.ru

DOI: 10.17212/2782-2230-2024-2-55-68

Ensuring the security of personal data in the enterprise information system*

N.E. Karpova[1], A.A. Babinova[2]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, associate professor of the electronic systems and information security department. E-mail: esib@samgtu.ru*
[2] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, assistant of the department of Applied Mathematics and Computer Science. E-mail: anyuta.babinova2000@yandex.ru*

With the modern development of information technologies, resources and computerization of society all over the world, in each of the spheres of human activity is not done without information technologies. Some of them are unique and generate income by their uniqueness, and as a result, one of the most urgent problem becomes the provision of information security in any organizations and enterprises, for any sphere and business activities.
Because people want to profit, they can commit criminal acts against the source of income that is always information. The most common source is personal data. In any organization or enterprise there are threats to the security of information that contains personal data. This information may be lost, copied, altered or blocked either by the perpetrator for profit or by mistake or negligence. Loss of confidential information can have both minor and very serious consequences. Therefore, personal data security plays an important role in maintaining and improving the activities of organizations, as it is a problem in all spheres of life.
This article discusses issues related to the development of a system to ensure the security of personal data in the enterprise's information system. During the implementation of the work, the regulatory acts in the field of protection and processing of personal data in the information system of the enterprise were analyzed, the analysis of the existing means of protection and initial protection of IPSDN was made.
As a result of the work, a system for the protection of personal data in IPDS was developed. Technical and organizational measures were selected and the equipment for the security system was validated.

Keywords: Personal data, Confidential information, Personal data information system, Information technologies, Basic security, Actual threats, Intruder, Security measures, Security system

REFERENCES

1. Convention on the Protection of Natural Persons in the Automated Processing of Personal Data (Strasbourg, 28 January 1981). *Konsul'tantPlyus*. (In Russian). Available at: http:///ww.consultant.ru/document/cons_doc_LAW_121499/ (accessed 30.05.2024).

* *Received 20 April 2024.*

2. Federal Law of the Russian Federation of July 27, 2006 No. 152-FZ "About personal data". *Konsul'tantPlyus*. (In Russian). Available at: http:///www.consultant.ru/document/cons_doc_LAW_61801/ (accessed 30.05.2024).

3. Federal Law of the Russian Federation of July 27, 2011. "On amendments to the Federal Law “About Personal Data”". *Konsul'tantPlyus*. (In Russian). Available at: https://www.consultant.ru/document/cons_doc_LAW_117437/ (accessed 30.05.2024).

4. Federal Law of the Russian Federation of July 27, 2006 No. 149-FZ "On information, information technologies and on information protection". *Konsul'tantPlyus*. (In Russian). Available at: http:////ww.consul.tant.ru/document/cons_doc_LAW_61798/ (accessed 30.05.2024).

5. Order of FSTEC of Russia No. 21 dated 18.02.2013 "On approval of the composition and content of organizational and technical measures to ensure security of personal data during their processing in personal data information systems". *FSTEC of Russia*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 30.05.2024).

6. Resolution of the Government of the Russian Federation from 15.09.2008 No. 687 "On approval of the Regulation on the features of the processing of personal data carried out without the use of automation means". *Garant.Ru*: web-site. (In Russian). Available at: https://base.garant.ru/193875 (accessed 30.05.2024).

7. Methodological document of the FSTEC of Russia dated February 05, 2021 "Methods of assessment of threats to information security". *FSTEC of Russia*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed 30.05.2024).

8. Methodological document of the FSTEC of Russia dated February 14, 2008 "Methods of identification of actual threats of security of personal data during their processing in information systems of personal data". *FSTEC of Russia*. (In Russian). Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodika-ot-14-fevralya-2008-g (accessed 30.05.2024).

9. Gavryushchenko A.P., Maslennikov A.V. O metodike opredeleniya aktual'nykh ugroz informatsionnoi bezopasnosti s ispol'zovaniem BDU FSTEK [On the methodology for determining current threats to information security using the FSTEC databas]. *Auditorium*, 2022, no. 2 (34), pp. 37–43. (In Russian).

10. State Register of Certified Means of Information Protection. *FSTEC of Russia*. (In Russian). Available at: https://reestr.fstec.ru/reg3 (accessed 30.05.2024).

11. *Secret Net Studio 8.5. Rukovodstvo administratora. Nastroika i ekspluatatsiya* [Secret Net Studio 8.5. Administrator's manual. Settings and operation]. Moscow, Kod bezopasnosti Publ., 2019. 106 p.

12. *Secret Net Studio 8.5. Rukovodstvo administratora. Lokal'naya zashchita* [Secret Net Studio 8.5. Admin Guide. Local Security]. Moscow, Kod bezopasnosti Publ., 2019. 159 p.

13. Isaev A.S., Khlyupina E.A. *Pravovye osnovy organizatsii zashchity personal'nykh dannykh* [Legal framework for personal data protection organization]. St. Petersburg, ITMO University Publ., 2014. 106 p. Available at: https://books.ifmo.ru/file/pdf/1570.pdf (accessed 30.05.2024).

14. Slepov O. *Zashchita personal'nykh dannykh* [Protection of personal data]. Available at: https://ww.jetinfo.ru/zaschita-personalnykh/ru (accessed 30.05.2024).

15. Basic model of threats to the security of personal data during their processing in personal data information systems (Extract) (approved by the FSTEC of Russia in 15.02.2008). *Konsul'tantPlyus*. (In Russian). Available at: http://www.consultant.ru/document/cons_doc_LAW_99662 (accessed 30.05.2024).

Для цитирования:

Карпова Н.Е., Бабинова А.А. Обеспечение безопасности персональных данных в информационной системе предприятия // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 55–68. – DOI: 10.17212/2782-2230-2024-2-55-68.

For citation:

Karpova N.E., Babinova A.A. Obespechenie bezopasnosti personal'nykh dannykh v informatsionnoi sisteme predpriyatiy [Ensuring the security of personal data in the enterprise information system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 55–68. DOI: 10.17212/2782-2230-2024-2-55-68.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 69–78

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-69-78

УГРОЗА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ФИШИНГА В СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

Н.Е. КАРПОВА[1], И.И. ВОСКАНЯН[2]

[1] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность». E-mail: esib@samgtu.ru*
[2] *443071, РФ, г. Самара, ул. Конноармейская, 17, инженер ООО «Газинформсервис». E-mail: naynaksov@gmail.com*

Информация – важнейший ресурс любой компании в наше время, поэтому обеспечение ее защиты является одной из приоритетных бизнес-задач каждой организации.
С течением времени технические системы защиты всё больше и больше совершенствуются за счет развития технологий, учета множества каналов утечек информации и увеличения потребности в обеспечении информационной безопасности в целом. Грамотно выстроенные технические системы защиты всегда будут выполнять возложенные на них задачи, но один-единственный фактор может сделать их бесполезными – это человек. Люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами и ошибками, являясь самым слабым звеном в цепочке безопасности.
Поэтому начали набирать популярность атаки, направленные не на саму систему, а на ее пользователей, так называемые социоинженерные атаки.
В настоящей статье рассмотрены вопросы угроз социальной инженерии и фишинга в современной информационной безопасности. Во время выполнения работы были проанализированы история и принцип работы социальной инженерии.
В результате работы был представлен пример настоящей фишинговой атаки (пентеста), произведен анализ статистических данных. Были представлены выводы об угрозе фишинга.

Ключевые слова: информационная безопасность, каналы утечки информации, пользователь, социальная инженерия, фишинг, угрозы, пентест, аттракция, система защиты

* Статья получена 29 апреля 2024 г.

ВВЕДЕНИЕ

Сейчас информация стала неотъемлемым и основополагающим ресурсом для любой компании. В связи с этим обеспечение безопасности информации стало одним из ключевых приоритетов всех организаций.

Качественные технические системы безопасности всегда будут выполнять свои задачи, однако их эффективность может быть подорвана одним фактором – человеком.

Поэтому эксплуатация «человеческого фактора» становится всё более популярной, так как позволяет обойти системы безопасности и сделать их бесполезными, попросту игрушками. Такой вид воздействия получил название «социальная инженерия».

Впервые в научном обороте понятие «социальная инженерия» было применено в СССР Алексеем Капитоновичем Гастевым – руководителем Центрального института труда (г. Москва), однако он рассматривал это понятие как науку, которая позволяет достичь максимальной производительности сотрудника на рабочем месте путем управления его психологическим состоянием.

Современная социальная инженерия эволюционировала в совокупность подходов прикладных социальных наук, ориентированных на целенаправленное изменение организационных структур, определяющих человеческое поведение [7].

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Обобщенный алгоритм атаки социального инженера в наши дни приведен на рис. 1.

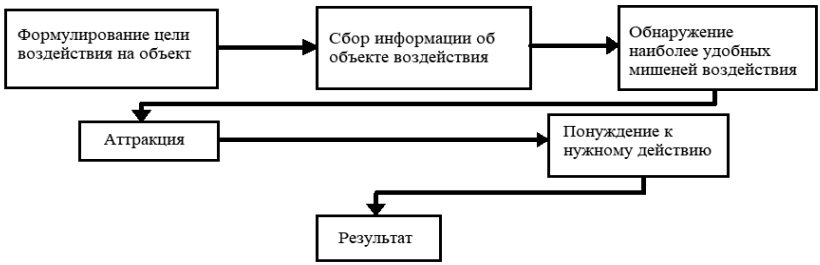


Рис. 1. Обобщенный алгоритм атаки социального инженера

Важнейшим аспектом атаки является аттракция (от лат. attrahere – привлекать, притягивать) – создание нужных условий для воздействия социоин-

женера на цель. Это включает в себя принуждение к желаемым действиям, когда объект воспринимает их как собственные и впоследствии принимает решение выполнить необходимые социоинженеру действия, думая, что они происходят по его собственной воле. То есть аттракция – это вхождение в доверие к жертве [4].

Существует множество разновидностей социальной инженерии – от так называемого «дорожного яблока» до «претекстинга», но, основываясь на статистике, которая приведена на рис. 2, наиболее распространенныи и опасными считаются фишинговые атаки.

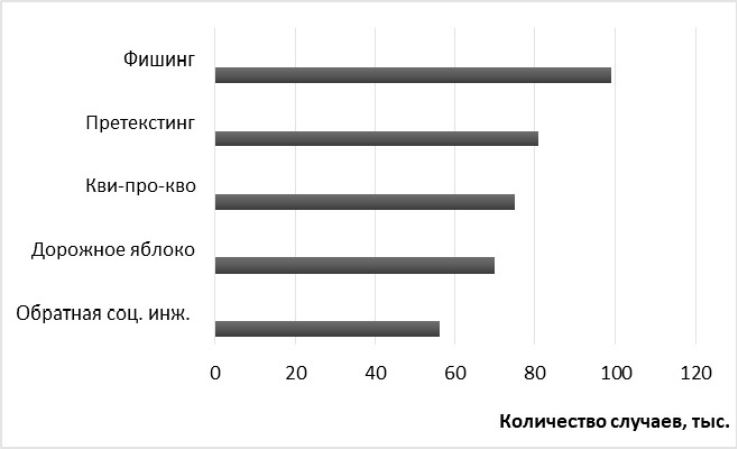


Рис. 2. Статистика атак социальной инженерии за 2021 год

Фишинг – это тип киберпреступления, при котором преступники выдают себя за надежный источник в Интернете, чтобы вынудить жертву передать им личную информацию (например, имя пользователя, пароль, номер банковской карты и пр.) [8].

В отличие от других интернет-угроз, фишинг не требует обладания высоким уровнем технического знания.

Фишинговые мошенники не пытаются использовать технические уязвимости в операционной системе устройства, вместо этого они прибегают к методам социальной инженерии. Нет ни одной операционной системы, которая бы обладала полной защитой от фишинга, несмотря на силу ее антивирусных средств. Фактически злоумышленники часто выбирают фишинг как метод, потому что не могут найти технические уязвимости. Зачем тратить время на взлом сложной системы защиты, когда можно обмануть пользователя и заста-

вить его добровольно раскрыть свои данные? В большинстве случаев самым уязвимым моментом в защите системы является не ошибка, затаенная глубоко в программном коде, а сам пользователь, который не обращает внимания на отправителя очередного электронного письма.

Фишинг имеет огромное разнообразие подходов, но общим аспектом всех атак является применение обмана с целью выманивания ценностей или информации.

Говоря о фишинге и о методах защиты от него, нельзя не упомянуть тестирование на проникновение (пентест). Это метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Анализ ведется с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. Цель испытаний на проникновение — оценить возможность его осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки. Результатом проведения испытания на проникновение, как правило, является отчет, содержащий выявленные в ходе анализа уязвимости и опционально рекомендации по их устранению [9].

ИССЛЕДОВАНИЕ

Рассмотрим типичную фишинговую атаку (пентест) на примере личного кабинета СамГТУ https://lk.samgtu.ru/:

Настоящая страница личного кабинета приведена на рис. 3.

Рис. 3. Настоящая страница личного кабинета

На рис. 4 приведена фишнговая страница.

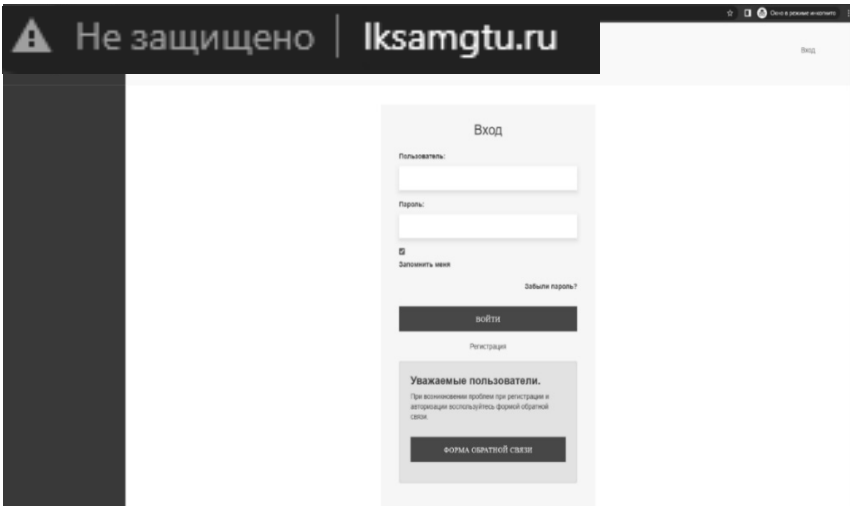


Рис. 4. Фишинговая страница личного кабинета

Письмо, содержащее аттракцию, представлено на рис. 5.

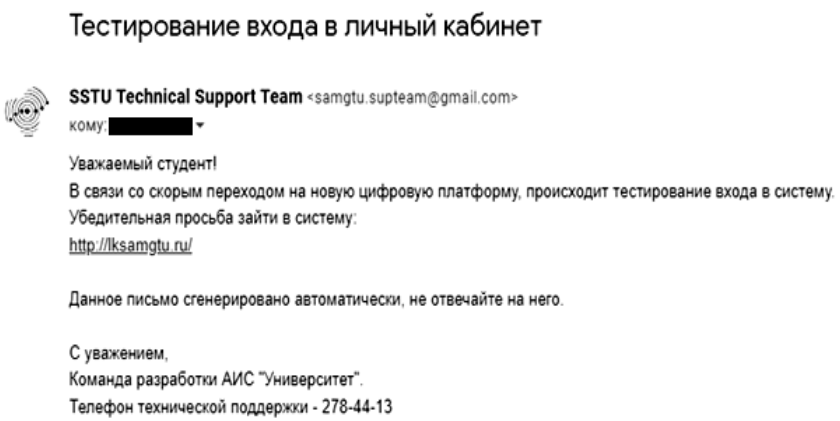


Рис. 5. Фишинговое электронное письмо

Такая, казалось бы, простейшая и банальная атака на студентов одного из крупнейших технических вузов страны выявила статистику, представленную на рис. 6.

Рис. 6. Статистика фишинговой атаки

Более половины испытуемых оказались уязвимы к фишинговой атаке и являются потенциальными жертвами социального инженера.

На основе фишинговых атак могут начинаться более сложные кибератаки, такие как заражение компьютеров, перехват управления технологическими процессами или нарушение работы системы. Поэтому сотрудники четко должны знать, как противостоять фишингу.

Основополагающим элементом для защиты от атак социальной инженерии являются пользователи с высоким уровнем знаний в области информационной безопасности, именно с ними нужно работать, чтобы обезопасить свою организацию.

Регулярные тестирования на проникновение с помощью тестовых фишинговых атак являются отличным методом для повышения уровня компетентности в области информационной безопасности сотрудников организации.

ЗАКЛЮЧЕНИЕ

Социальная инженерия как наука зародилась именно в нашей стране. Но ее функция отличалась от современной социальной инженерии. А.К. Гастев разработал и изучал эту науку, чтобы понять, как добиться максимальных результатов от сотрудников на их рабочем месте.

Социальная инженерия приобрела свой современный облик в 1980-х годах. С тех пор проблема подобных атак становится всё более серьезной. Появляются новые и изощренные методы и стратегии обмана самой сильной, но в то же время самой уязвимой системы – человека.

Самым распространенным методом атак социальной инженерии является фишинг. Каждый человек сталкивается с подозрительными электронными письмами, СМС-сообщениями или звонками. Ежегодно миллионы людей и тысячи организаций становятся жертвами фишинговых атак, что влечет за собой потерю миллионов долларов.

Угроза взлома, который нарушит секретность вашей жизни или информационной системы вашей компании, может казаться не настолько реальной, пока это не произойдет однажды. Чтобы избежать столь дорогостоящей дозы действительности, нам нужно стать осведомленными, образованными, бдительными и настойчиво защищать наши информационные активы, нашу собственную персональную информацию и наши национальные критичные инфраструктуры. И мы должны научиться этому уже сегодня.

СПИСОК ЛИТЕРАТУРЫ

1. *Гастев А.К.* Как надо работать: практическое введение в науку организации труда. – Изд. 2-е. – М.: Экономика,1972. – 478 с.

2. *Гастев А.К.* Социальные установки // У истоков НОТ: забытые дискуссии и нереализованные идеи. – Л., 1990. – С. 103.

3. *Гастев А.К.* Трудовые установки. – М.: Экономика, 1973. – 343 с.

4. *Генне О.В.* Заметки о социальной инженерии // Защита информации. Инсайд. – 2006. – № 6 (12). – С. 16–19.

5. *Митник К., Саймон У.* Искусство обмана. – М.: АйТи, 2004. – ISBN 5-98453-011-2. – ISBN 0-471-23712-4.

6. *Sammons J.* The basics of digital forensics: the primer for getting started in digital forensics. – Elsevier Science, 2012. – 177 p. – ISBN 9781597496612.

7. Инженерия социальная // Российская социологическая энциклопедия / под общ. ред. Г.В. Осипова. – М.: Норма–Инфра-М, 1999. – URL: https://sociologicheskaya.academic.ru/392 (дата обращения: 31.05.2024).

8. Все о фишинге. – URL: https://ru.malwarebytes.com/phishing/ (дата обращения: 31.05.2024).

9. *Музалевский Ф.А.* Что такое пентест? – URL: https://rtmtech.ru/articles/chto-takoe-pentest/ (дата обращения: 31.05.2024).

10. *Романов В.Г., Романова И.В.* Социальное мошенничество «COVID-19» и манипулятивные технологии социальной инженерии // Вестник Забайкальского государственного университета. – 2020. – Т. 26, № 9. – С. 57–67.

11. *Дьяков Н.В.* Применение методов социальной инженерии в социальных сетях // // Общество. – 2020. – № 2 (17). – С. 126–128.

12. *Румянцев Е.П., Найденов Н.Д.* Виды фишинга и способы защиты от него // Аллея науки. – 2018. – № 6 (22). – С. 451–455.

13. *Штайгер А.А.* Социальная инженерия на примере фишинга // Вестник современных исследований. – 2018. – № 6.3 (21). – С. 612–614.

14. 11 типов фишинга и примеры из реальной жизни. – URL: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/ (дата обращения: 31.05.2024).

15. Как избежать атаки с использованием социальной инженерии / Лаборатория Касперского. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (дата обращения: 31.05.2024).

Карпова Надежда Евгеньевна, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Основные направления научных исследований – автоматизированные интеллектуальные системы и автоматизированные информационно-измерительные системы. Имеет более 100 публикаций. E-mail: esib@samgtu.ru

Восканян Игит Игитович, инженер ООО «Газинформсервис». E-mail: naynaksov@gmail.com

DOI: 10.17212/2782-2230-2024-2-69-78

Threat of social engineering and phishing in modern information security*

N.E. Karpova[1], I.I. Voskanyan[2]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, associate professor of the electronic systems and information security department. E-mail: esib@samgtu.ru*
[2] *«Gazinform», 17 Konneramiyskaya Street, Samara, 443071, Russian Federation, engineer of «Gazinform». E-mail: naynaksov@gmail.com*

Information is the most important resource of any company in our time, so ensuring its protection is one of the priority business tasks of each organization.
Over the years, technical security systems have been increasingly improved through technological developments, the recording of multiple channels of information leakage and the growing need for information security in general. Well-designed technical protection systems will always perform the tasks assigned to them, but one single factor can make them useless – a person. People will remain human, with their weaknesses, prejudices, stereotypes and mistakes, being the weakest link in the security chain.
So attacks started to gain popularity, targeting not the system itself, but its users, the so-called social engineering attacks.
In this article the issues of threats of social engineering and phishing in modern information security are considered. During the work the history and principle of social engineering were analyzed.
As a result, an example of a real phishing attack (penteste) was presented, the analysis of statistical data was made. Conclusions about the phishing threat were presented.

Keywords: Information security, Information leakage channels, User, Social engineering, Phishing, Threats, Pentest, Attraction, Security system

REFERENCES

1. Gastev A.K. *Kak nado rabotat': prakticheskoe vvedenie v nauku organizatsii truda* [How to work. Practical introduction to the science of the organization of labor]. 2nd ed. Moscow, Ekonomika Publ., 1972. 478 p.

2. Gastev A.K. Sotsial'nye ustanovki [Social Attitudes]. *U istokov NOT: zabytye diskussii i nerealizovannye idei* [Origins of NOTE: Forgotten discussions and unrealized ideas]. Leningrad., 1990, p. 103.

3. Gastev A.K. *Trudovye ustanovki* [Industrious routine]. Moscow, Ekonomika Publ., 1973. 343 p.

4. Genne O.V. Zametki o sotsial'noi inzhenerii [Notes on social engineering]. *Zashchita informatsii. Insaid*, 2006, no. 6 (12), pp. 16–19. (In Russian).

* *Received 29 April 2024.*

5. Mitnick K., Simon W. *Iskusstvo obmana* [Art of deception]. Moscow, AiTi Publ., 2004. ISBN 5-98453-011-2. ISBN 0-471-23712-4. (In Russian).

6. Sammons J. *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier Science, 2012. 177 p. ISBN 9781597496612.

7. Inzheneriya sotsial'naya [Engineering social]. *Rossiiskaya sotsiologicheskaya entsiklopediya* [Russian sociological encyclopedia]. Moscow, Norma–Infra-M Publ., 1999. Available at: https://sociologicheskaya.academic.ru/392 (accessed 31.05.2024).

8. *All about Phishing*. Available at: https://www.malwarebytes.com/phishing (accessed 31.05.2024).

9. Muzalevskii F.A. *Chto takoe pentest?* [What is pentest?]. Available at: https://rtmtech.ru/articles/chto-takoe-pentest/ (accessed 31.05.2024).

10. Romanov V.G., Romanova I.V. Sotsial'noe moshennichestvo «COVID-19» i manipulyativnye tekhnologii sotsial'noi inzhenerii [Social fraud-covid-19 and manipulative social engineering technologies]. *Vestnik Zabaikal'skogo gosudarstvennogo universiteta = Transbaikal State University Journal*, 2020, vol. 26, no. 9, pp. 57–67.

11. Dyakov N.V. Primenenie metodov sotsial'noi inzhenerii v sotsial'nykh setyakh [Application of social engineering methods in social networks]. *Obshchestvo = Society*, 2020, no. 2 (17), pp. 126–128.

12. Rumyantsev E.P., Naidenov N.D. Vidy fishinga i sposoby zashchity ot nego [Types of phishing and ways of protection against it]. *Alleya nauki = Alley of Science*, 2018, no. 6 (22), pp. 451–455.

13. Shtaiger A.A. Sotsial'naya inzheneriya na primere fishinga [Social engineering by example of phishing]. *Vestnik sovremennykh issledovanii*, 2018, no. 6.3 (21), pp. 612–614. (In Russian).

14. *11 tipov fishinga i primery iz real'noi zhizni* [11 types of phishing + real-life examples]. Available at: https:///www.cloudav.ru/mediacenter/tips/tips/types-of-phishing/ (accessed 31.05.2024).

15. Kaspersky Lab. *Kak izbezhat' ataki s ispol'zovaniem sotsial'noi inzhenerii* [How to avoid an attack using social engineering]. Available at: https://ww.kaspersky.ru/resource-center/threats/how--avoid-social-engeringattacks (accessed 31.05.2024).

Для цитирования:

Карпова Н.Е., Восканян И.И. Угроза социальной инженерии и фишинга в современной информационной безопасности // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 69–78. – DOI: 10.17212/2782-2230-2024-2-69-78.

For citation:

Karpova N.E., Voskanyan I.I. Ugroza sotsial'noi inzhenerii i fishinga v sovremennoi informatsionnoi bezopasnosti [Threat of social engineering and phishing in modern information security]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 69–78. DOI: 10.17212/2782-2230-2024-2-69-78.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 79–89

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 519.24 DOI: 10.17212/2782-2230-2024-2-79-89

РАЗРАБОТКА ОНЛАЙН-СЕРВИСА ДЛЯ ОБРАБОТКИ ИНФОРМАЦИИ О ПРОВЕРКЕ ЗНАНИЙ СОТРУДНИКОВ КОМПАНИИ*

Г.В. ТРОШИНА[1], А.С. КАЛИНКИНА[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, бакалавр кафедры вычислительной техники E-mail: arianakalinkina@mail.ru*

В современных условиях компаниям приходится сталкиваться с большой конкуренцией в быстро растущих сегментах отрасли или областях рынка. Именно поэтому в бизнес-среде управление знаниями сотрудников является ключевой задачей. Организации уделяют время не только обучению персонала, но и отработке теоретических знаний на практике, разбору ошибок, которые возникают во время общения с клиентом. Компаниям необходимо искать эффективные методы оценки знаний своих сотрудников в целях повышения конкурентоспособности, но существующие платформы не предоставляют всех необходимых возможностей. Поэтому появляется необходимость в создании узконаправленного программного обеспечения, которое бы давало возможность формировать тесты для проверки знаний работников организации и анализировать полученные результаты. В настоящей статье представлены основные этапы создания онлайн-сервиса для обработки информации о результатах тестирования знаний сотрудников компании. Каждый сотрудник имеет доступ в свой личный кабинет, в котором он может выполнять тесты, отслеживать результаты и рейтинг среди других сотрудников по среднему баллу, получить обратную связь от руководителя. У руководителя компании имеется возможность отслеживать информацию по каждому сотруднику, назначать тесты, комментировать ответы, а также удалять или добавлять новых сотрудников. При создании тестов предусмотрена возможность выбрать тип вопроса, в том числе осуществлять загрузку аудиофайлов и изображений. Создана удобная панель меню, которая содержит разнообразные вкладки, соответствующие роли пользователя. Разработана база данных и определены типы связей между таблицами. Созданы учетные записи пользователей для назначения соответствующих уровней доступа.

Ключевые слова: база данных, онлайн-сервис, права доступа, пользователь базы данных, оценка знаний, таблица, тест, обработка информации

* Статья получена 07 марта 2024 г.

ВВЕДЕНИЕ

Для успешной работы компании «6F Wear», которая занимается производством повседневной одежды и спортивной экипировки, очень важно иметь сильную и обученную команду менеджеров, от которой зависит количество и качество продаж, что напрямую влияет на прибыль компании. Поэтому важно уделять большое внимание обучению сотрудников и затем закреплять полученные ими знания на тестах, которые включают в себя различные типы вопросов. Основной навык, которым должны обладать менеджеры, – это продажа услуг во время разговора с клиентом. Менеджер должен владеть всей информацией о компании: предоставляемые услуги, типы одежды и экипировки, цены на услуги, дизайн, используемый текстиль. В том числе менеджерам важно обладать отличными навыками коммуникации. Проверка знаний сотрудников необходима для увеличения количества продаж товаров компании, а это возможно при улучшении компетенций сотрудников компании.

Таким образом, необходимо реализовать онлайн-сервис, который предоставит возможность руководителю создавать тесты для сотрудников, отслеживать их результаты, писать комментарии по открытым вопросам, просматривать рейтинг по каждому сотруднику. Сотрудник компании должен иметь возможность решать тесты, просматривать комментарии от руководителя, отслеживать свои результаты и рейтинг.

1. РАЗРАБОТКА БАЗЫ ДАННЫХ

В рамках разрабатываемого проекта был выбран язык PHP для разработки серверной части онлайн-сервиса. Язык PHP является оптимальным выбором, так как обеспечивает простоту разработки, хорошую поддержку и широкий выбор инструментов для реализации данного проекта [1–4]. Ниже приведены основные достоинства использования языка PHP.

1. Простота и скорость разработки: PHP имеет простой синтаксис и широко используется в веб-разработке, особенно для создания динамических веб-сайтов и приложений. Это делает его привлекательным для небольших проектов с ограниченным бюджетом и временем.

2. Обширная документация и сообщество: PHP имеет обширную документацию и огромное сообщество разработчиков. Это означает, что можно легко найти ответы на вопросы, а также множество готовых решений и библиотек для реализации различных функций проекта.

3. Поддержка баз данных: PHP имеет широкую поддержку различных баз данных, таких как MySQL, PostgreSQL, SQLite и другие. Это позволяет легко взаимодействовать с базой данных для хранения информации.

4. Процедурный и объектно ориентированный подход: PHP поддерживает как процедурное, так и объектно ориентированное программирование. Это дает возможность выбрать подход, который лучше всего подходит для проекта, основываясь на его размере и сложности.

Выбор базы данных играет критическую роль в разработке веб-приложений, поскольку база данных является фундаментальным компонентом, обеспечивающим хранение, управление и доступ к данным, которые используются приложением [5–9].

На рис. 1 приведена структура разработанной базы данных.

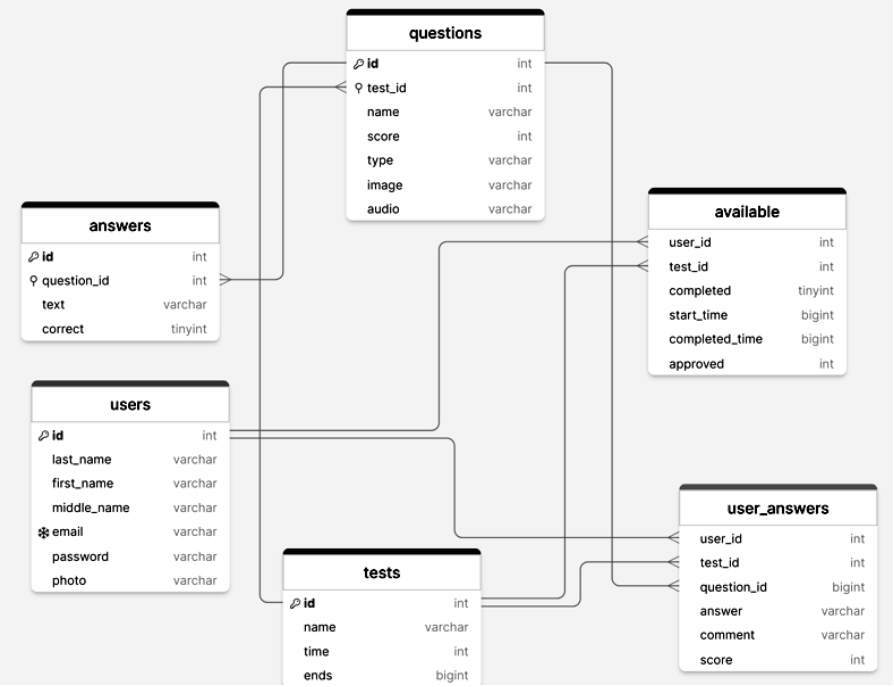


Рис. 1. Структура базы данных

Fig. 1. Database structure

База данных влияет на производительность, масштабируемость, безопасность и надежность любого веб-приложения. В рамках этой разработки используется одна из самых популярных и функциональных систем управления базами данных MySQL, что позволяют просто и эффективно выполнять

любые запросы, читать и записывать данные, обрабатывать ошибки. В работе с MySQL основное внимание уделяется созданию таблиц и определению связи между ними для хранения данных [1, 10]. MySQL может обрабатывать различные типы данных, такие как изображения, заметки, задачи, аудио- и текстовые файлы, и поддерживать связи между ними. PhpMyAdmin представляет собой инструмент, используемый для управления базой данных MySQL. В работе [11] даны рекомендации по реализации профессиональных компетенций в образовательном процессе.

Потенциальными пользователями разработанного онлайн-сервиса являются сотрудники и руководители компании.

Ниже описываются таблицы, входящие в разработанную базу данных. Таблица Answers содержит данные о вариантах ответов на вопросы:

- id – уникальный идентификатор ответа;
- question_id – идентификатор вопроса, к которому относится ответ;
- text – текст ответа;
- correct – флаг, указывающий, является ли ответ правильным (0 – неправильный, 1 – правильный).

Таблица Available хранит информацию о доступных пользователям тестах:

- user_id – идентификатор пользователя;
- test_id – идентификатор теста;
- completed – флаг, указывающий, завершен ли тест (0 – не завершен, 1 – завершен);
- start_time – время начала теста;
- completed_time – время завершения теста;
- approved – флаг, указывающий, одобрен ли тест (0 – не одобрен, 1 и выше – одобрен).

В таблице Questions находятся данные о вопросах в тестах:

- id – уникальный идентификатор вопроса;
- test_id – идентификатор теста, к которому относится вопрос;
- name – текст вопроса;
- score – количество баллов за вопрос;
- type – тип вопроса;
- image – изображение, связанное с вопросом (необязательно);
- audio – аудиофайл, связанный с вопросом (необязательно).

В таблице Tests содержится информация о тестах:

- name – название теста;
- time – продолжительность теста в минутах;
- ends – время завершения теста.

Таблица Users – таблица, хранящая информацию о пользователях системы:

- id – уникальный идентификатор пользователя;
- last_name – фамилия пользователя;
- first_name – имя пользователя;
- middle_name – отчество пользователя (необязательно);
- email – адрес электронной почты пользователя (уникальный);
- password – хэш пароля пользователя;
- photo – фотография пользователя (необязательно).

В таблице User_answers находятся ответы пользователей на вопросы тестов:

- user_id – идентификатор пользователя;
- test_id – идентификатор теста;
- question_id – идентификатор вопроса;
- answer – ответ пользователя;
- comment – комментарий к ответу;
- score int – количество баллов за ответ.

2. ОПИСАНИЕ РОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ

Для работы с онлайн-сервисом по проверке знаний сотрудников компании используется роль администратора и роль пользователя.

На рис. 2 приведена диаграмма прецедентов.

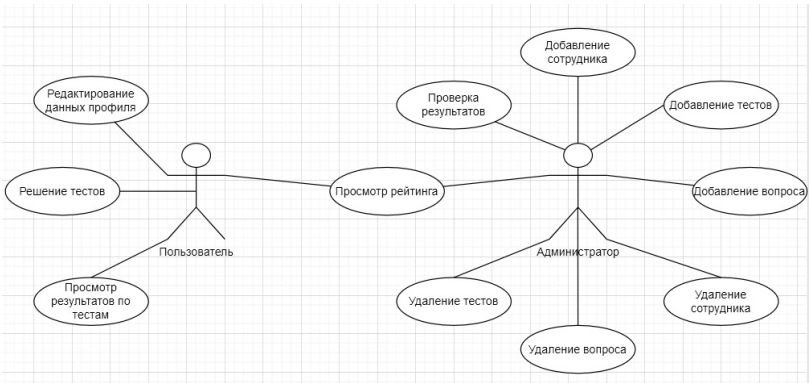


Рис. 2. Диаграмма прецедентов

Fig. 2. The precedents diagram

Пользователь – сотрудник, который решает тесты. Его регистрирует администратор при помощи адреса электронной почты, после чего пользователю приходит уведомление с временным паролем, который можно поменять на постоянный пароль. Для пользователя предусмотрена возможность менять такие данные своего профиля, как, например, фамилия, имя, отчество, адрес электронной почты, пароль, загрузить фото при необходимости. Пользователь решает тесты, просматривает результаты по ним, а также просматривает рейтинг по результатам тестирований всех сотрудников.

Администратор – руководитель отдела, который регистрирует сотрудников в системе, назначает им тесты и проверяет их. Администратор имеет возможность добавлять / удалять сотрудников, добавлять / удалять тесты и вопросы, устанавливает ограничения. Администратор просматривает результаты тестов по каждому сотруднику, выставляет баллы по открытым вопросам, оставляет комментарии, просматривает рейтинг каждого сотрудника по результатам тестов.

3. ТЕХНОЛОГИЯ РАБОТЫ ПОЛЬЗОВАТЕЛЯ

Внутри меню для пользователя представлены различные разделы, такие как «Профиль», «Тесты», «Результаты», «Рейтинг» и «Выход». Для администратора отображаются разделы «Тесты», «Сотрудники», «Результаты», «Рейтинг» и «Выход».

На рис. 3 приведен раздел «Сотрудники».

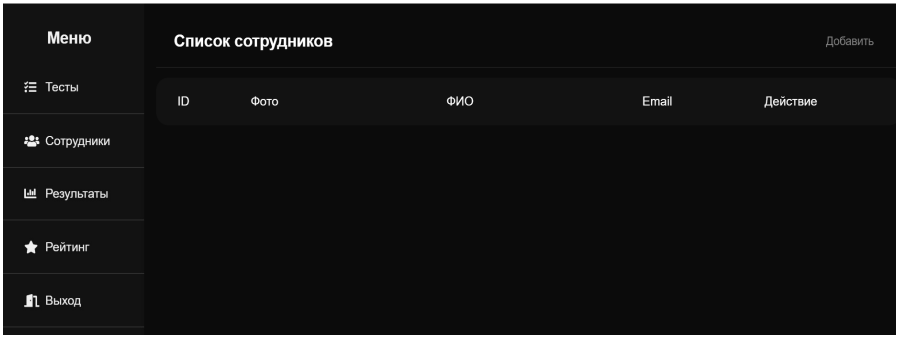


Рис. 3. Раздел «Сотрудники»

Fig. 3. Section «Employees»

Для добавления сотрудников нажимаем кнопку «Добавить», которая находится в верхнем правом углу. Указываем данные по нашему новому пользователю – фамилию, имя, отчество и e-mail и добавляем сотрудника. На рис. 4 приведен результат добавления нового сотрудника.

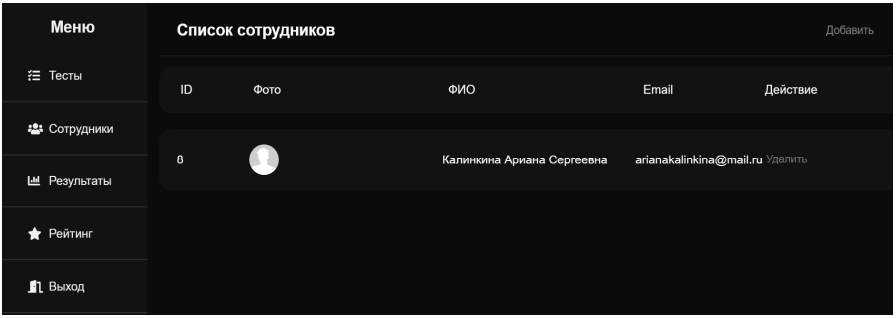


Рис. 4. Добавление сотрудника

Fig. 4. Add employee

Для добавления теста с вопросами необходимо перейти в раздел «Тесты» и нажать кнопку «Создать» (рис. 5).

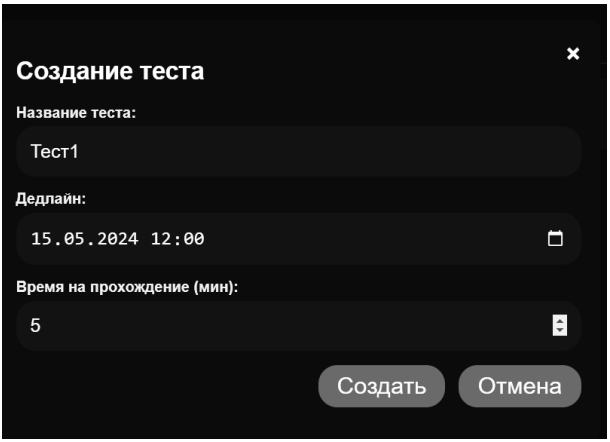


Рис. 5. Создание теста

Fig. 5. Test creating

Администратор назначает тесты сотрудникам, ограничивая время выполнения, а также устанавливая крайний срок для его решения.

ЗАКЛЮЧЕНИЕ

В настоящей статье представлен онлайн-сервис, предназначенный для проверки знаний сотрудников компании. Разработана структура базы данных, включая определение сущностей, их атрибутов и связей. Выполнена настройка взаимодействия базы данных с веб-приложением, а также настройка интерфейса для различных ролей пользователей. Результаты тестов сохраняются в системе. Руководитель компании осуществляет проверку знаний сотрудников и контролирует результаты тестирования. Каждый пользователь имеет доступ в свой личный кабинет, где он просматривает назначенные тесты, решает их, отслеживает статус проверки.

СПИСОК ЛИТЕРАТУРЫ

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

2. *Дронов В.А.* PHP 5/6, MySQL 5/6 и Dreamweaver CS4. Разработка интерактивных Web-сайтов. – СПб.: БХВ-Петербург, 2009. – 534 с.

3. Руководство по PHP. – URL: http://www.php.net/manual/ru (дата обращения: 31.05.2024).

4. 7 лучших инструментов разработки на PHP для веб-разработки в 2022 году // Веб-студия WRP. – URL: https://wrp.ru/statii/7-luchshikh-instrumentov-razrabotki-na-php-dlya-veb-razrabotki-v-2022-godu/ (дата обращения: 31.05.2024).

5. *Гарсиа-Молина Г., Ульман Д.Д., Уидом Д.* Системы баз данных: полный курс: пер. с англ. – М.: Вильямс, 2003. – 1088 с.

6. *Малыхина М.П.* Базы данных: основы, проектирование, использование. – СПб.: БХВ-Петербург, 2004. – 512 с.

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

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

9. *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.

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

11. *Romanov E.L., Troshina G.V., Yakimenko A.A.* Software engineering for industry specialists // Proceedings of the 4th International Technologies in Engineering Education, Moscow, 23–26 Oct. 2018. – 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

Калинкина Ариана Сергеевна, бакалавр кафедры вычислительной техники Новосибирского государственного технического университета. Направления научных исследований – базы данных, информационные технологии. E-mail: arianakalinkina@mail.ru

DOI: 10.17212/2782-2230-2024-2-79-89

Development of an online service for processing data on testing the knowledge of company employees*

G.V. Troshina[1], A.S. Kalinkina[2]

[1].*Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, candidate of Technical Sciences, 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, bachelor of the computer engineering department. E-mail: arianakalinkina@mail.ru*

In today's environment, companies have to face great competition in rapidly growing industry segments or market areas. This is why managing employee knowledge is key task in a business environment. Organizations devote time not only to training personnel, but also to working out theoretical knowledge in practice, analyzing errors that arise during communication with the client. Companies need to look for effective methods to assess their employees' knowledge in order to increase competitiveness, but existing platforms do not provide all the necessary opportunities. Therefore, there is a need to create highly targeted software that would make it possible to form tests for the knowledge assessment of organization employees and analyze the results obtained. This article presents the main stages of an online service creating for the information processing about the testing results of the company employees knowledge. Each employee has access to his personal account, in which he can perform tests, track results and rating among other employees by average score, and receive feedback from

* *Received 07 March 2024.*

the manager. The head of the company has the ability to track information for each employee, assign tests, comment on answers, and delete or add new employees. When creating tests, it is possible to select the question type, including downloading audio files and images. The convenient menu bar has been created, which contains various tabs corresponding to the user role. The database has been developed and the relationships types between tables have been defined. User accounts have been created to assign appropriate access levels.

Keywords: database, online service, access rights, database user, knowledge assessment, table, test, information processing

REFERENCES

1. Davis M.E., Phillips J.A. *Izuchaem PHP i MySQL* [Learning PHP and MySQL]. St. Petersburg, Simvol-plyus Publ., 2008. 260 p. (In Russian).

2. Dronov V.A. *PHP 5/6, MySQL 5/6 i Dreamweaver CS4. Razrabotka interaktivnykh Web-saitov* [PHP 5/6, MySQL 5/6 and Dreamweaver CS4. Interactive websites]. St. Petersburg, BHV-Peterburg Publ., 2009. 534 p.

3. *PHP Manual*. Available at: https://www.php.net/manual/en (accessed 31.05.2024).

4. 7 luchshikh instrumentov razrabotki na PHP dlya veb-razrabotki v 2022 godu. *Veb-studiya WRP* [Web studio WRP]. Available at: https://wrp.ru/statii/7-luchshikh-instrumentov-razrabotki-na-php-dlya-veb-razrabotki-v-2022-godu/ (accessed 31.05.2024).

5. Garcia-Molina H., Ullman J.D., Widom J. *Sistemy baz dannykh: polnyi kurs* [Database system: the complete book]. Moscow, Vil'yams Publ., 2003. 1088 p. (In Russian).

6. Malykhina M.P. *Bazy dannykh: osnovy, proektirovanie, ispol'zovanie* [Databases: basics, design, use]. St. Petersburg, BHV-Peterburg Publ., 2004. 512 p.

7. 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.

8. Connolly T., Begg C. *Bazy dannykh: proektirovanie, realizatsiya i soprovozhdenie* [Database systems: a practical approach to design, implementation, and management]. Moscow, Vil'yams Publ., 2003. 1436 p. (In Russian).

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

10. Gol'tsman V. *MySQL 5.0*. St. Petersburg, Piter Publ., 2010. 370 p.

11. Romanov E.L., Troshina G.V., Yakimenko A.A. Software engineering for industry specialists. *Proceedings of the 4th International Technologies in Engineering Education*, Moscow, 23–26 Oct. 2018. IEEE, 2018, pp. 222–225.

Для цитирования:

Трошина Г.В., Калинкина А.С. Разработка онлайн-сервиса для обработки информации о проверке знаний сотрудников компании // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 79–89. –DOI: 10.17212/2782-2230-2024-2-79-89.

For citation:

Troshina G.V., Kalinkina A.S. Razrabotka onlain-servisa dlya obrabotki informatsii o proverke znanii sotrudnikov kompanii [Development of an online service for processing data on testing the knowledge of company employees]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 79–89. DOI: 10.17212/2782-2230-2024-2-79-89.

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.