ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056

Технологические аспекты обеспечения информационной безопасности в организациях

Н.Н. Чибинев, С.Р. Федосеев, А.Н. Павлов
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г. Новочеркасск, Российская Федерация

Аннотация
Данное исследование проблемы информационной безопасности учитывает последствия кибератак на технологические системы производственных объектов. Выявлены уязвимости и защитные меры, которые удалось обойти злоумышленникам. Использовались методы обобщения, обработки и анализа статистических данных о чрезвычайных ситуациях. Работа фокусируется на выявлении ключевых причин реализованных атак и оценке эффективности технологических методов обеспечения безопасности.
Выявлены такие типичные уязвимости, как недостаточная сетевая сегментация, использование устаревших систем и слабые аутентификационные меры. Проанализированы причины успешных атак: недостаточное осознание рисков и отсутствие системы мониторинга и реагирования.
Отмечены современные технологические решения, призванные обеспечить безопасность информационных систем. Речь идет о криптографии, идентификации и системе мониторинга. В заключении указывается на необходимость определения на законодательном уровне правовых и организационных основ борьбы с чрезвычайными ситуациями в области информационной безопасности.

Ключевые слова: атака программы-вымогателя, сетевая сегментация, неустранимые уязвимости, реагирование на киберугрозы, компетентность персонала в области кибербезопасности

Для цитирования. Чибинев Н.Н., Федосеев С.Р., Павлов А.Н. Технологические аспекты обеспечения информационной безопасности в организациях. *Молодой исследователь Дона.* 2024;9(1):32–34.

Technological Aspects of Information Security in Organizations

Nikolai N. Chibinev, Stanislav R. Fedoseev, Aleksandr N. Pavlov
Platov South-Russian State Polytechnic University (NPI), Novocherkassk, Russian Federation

Abstract
This study of the problem of information security takes into account the consequences of cyberattacks on technological systems of production facilities. The consequences of cyberattacks were analyzed, vulnerabilities and protective measures that the attackers managed to circumvent were identified. Methods of generalization, processing and analysis of statistical data on emergency situations were used. The study focuses on identifying the key causes of implemented attacks and assessing the effectiveness of technological methods in ensuring security.
Common vulnerabilities identified include insufficient network segmentation, use of outdated systems, and weak authentication measures. The reasons for successful attacks were analyzed: insufficient awareness of risks and the lack of a monitoring and response system.
Modern technological solutions designed to ensure the security of information systems are noted. It concerns cryptography, identification and monitoring system. In conclusion, the question is raised about the need to define at the legislative level the legal and organizational framework for combating emergency situations in the field of information security.

Keywords: ransomware attack, network segmentation, unfixable vulnerabilities, response to cyber threats, personnel competence in the field of cybersecurity

For citation. Chibinev NN, Fedoseev SR, Pavlov AN. Technological Aspects of Information Security in Organizations. *Young Researcher of Don.* 2024;9(1):32–34.

Введение. В компьютерной системе разрушающее программное средство может некоторое время оставаться незамеченным. Его нередко программируют таким образом, что вредоносное действие активируется при наступлении определенного события, даты или свершения некоторых операций. Весьма трудно понять и предсказать логику развития атаки до того, как разрушающее программное средство себя проявит.

Цель данного исследования — анализ технологических аспектов обеспечения информационной безопасности на производственных объектах и в организациях с акцентом на шифрование данных и коммуникаций, аутентификацию и авторизацию, мониторинг и анализ безопасности, а также защиту от вредоносных программ.

Для решения поставленной задачи авторы обобщили, обработали и проанализировали статистические данные о чрезвычайных ситуациях, связанных с кибератаками и утечками данных на производственных объектах. Использовались методы сплошного и выборочного исследования.

Основная часть. Целями киберугроз могут быть, в частности, информационные системы производственных предприятий и государственных организаций. Особый интерес для злоумышленников представляют объекты, критически важные с точки зрения национальных интересов. Атаки на информационные системы опасных производственных объектов и государственных учреждений могут обернуться чрезвычайными ситуациями и катастрофами.

Один из примеров такой чрезвычайной ситуации — результат атаки программы-вымогателя 8 февраля 2023 года в городе Модесто округа Станисло, штат Калифорния, США [1]. Хакерам удалось на несколько дней отключить IT-систему полицейского управления, и в течение этого времени правоохранители не могли оперативно реагировать на правонарушения.

3 марта 2023 года на встрече с молодыми учеными, изобретателями и технологическими предпринимателями Евразийского НОЦ в Уфе вице-премьер России Д.Н. Чернышенко сообщил, что в 2022 году отражено около 50 тыс. атак на российские интернет-ресурсы, в 2023 году число кибератак на российские системы выросло на 65 %. Отмечено, что в 2021 году целью атак был финансовый сектор, а в 2022-м — государственный [2]. После начала специальной военной операции центр информационной безопасности ФСБ ежедневно регистрирует более 170 кибератак [3].

22 и 28 февраля 2023 года из-за хакерских атак на инфраструктуру связи МЧС РФ в эфире радиостанций некоторых российских регионов (в частности, в Крыму, Белгородской и Воронежской областях) неоднократно объявлялась ложная воздушная тревога [4]. В связи с этим МЧС России перенесло комплексные проверки систем оповещения населения с 1 марта на 4 октября 2023 года.

Авторы представленной работы проанализировали исследования, которые проводили эксперты в области кибербезопасности. В их числе были инженеры по безопасности информационных систем, специалисты по анализу угроз и по восстановлению после инцидентов. В последнем случае задействовали средства мониторинга сетевого трафика, инструменты цифровой форензики[1] и системы обнаружения вторжений для анализа последствий кибератак, нацеленных на технологические системы производственных объектов. Изыскания позволили выявить перечисленные ниже типичные уязвимости и нарушенные уровни защиты.

1. Слабая сетевая сегментация. В некоторых случаях производственные сети были недостаточно отделены от корпоративных, что позволило злоумышленникам, получив один уровень доступа, открыть следующий.

2. Устаревшие системы и программное обеспечение. Использование неактуального софта с неустранимыми уязвимостями облегчало взлом.

3. Слабые аутентификационные меры. Отсутствие двухфакторной аутентификации или использование слабых паролей упрощало задачу злоумышленникам.

4. Необновляемые элементы. Продолжительное использование устройств с истекшими сроками обновлений, без патчей также открывает уязвимости систем.

Исследование позволило выявить основные причины реализованных кибератак на технологические системы производственных объектов.

1. Недостаточное осознание рисков. Многие организации недооценивают угрозы кибербезопасности и не принимают адекватные меры предосторожности.

2. Отсутствие системы мониторинга и реагирования. Большинство организаций не имели эффективных систем мониторинга и быстрого реагирования на киберугрозы.

3. Недостаточное внимание к персоналу. Социальная инженерия и фишинг оказались успешными из-за низкой компетентности персонала в области кибербезопасности.

4. Слабые политики безопасности. Отсутствие актуальных и строгих политик безопасности позволило злоумышленникам скрытно проводить вредоносные операции.

Заключение. Анализ проблем корпоративной кибербезопасности позволяет сделать ряд заключений.

[1] Сбор, анализ и интерпретация цифровых данных с целью выявления и расследования киберпреступлений или инцидентов безопасности.

1. Для обеспечения информационной безопасности следует задействовать такие инструменты, как криптография, идентификация и аутентификация, брандмауэры и системы обнаружения вторжений. Технологические решения для управления информационной безопасностью: системы управления доступом, средства мониторинга, аудита и облачные технологии.

2. Необходимо постоянно поддерживать систему управления рисками и повышать компетентность сотрудников в сфере информационной безопасности.

3. Для производственных объектов и организаций следует сформировать модель угроз технологической безопасности программного обеспечения. Это официально принятый корпоративный нормативно-технический документ, которым обязаны руководствоваться заказчики и разработчики программных комплексов.

4. Необходим международный законодательный документ, определяющий правовые и организационные основы борьбы с чрезвычайными ситуациями информационного характера.

5. С 1 января 2025 года нужно прекратить использование иностранного программного обеспечения на объектах критической инфраструктуры, принадлежащей госорганам. Этого требует Указ Президента № 166 от 30.03.2022 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [5].

Список литературы

1. *Город Окленд в США объявил режим ЧС после кибератаки*. URL: https://www.securitylab.ru/news/536498.php (дата обращения: 25.12.2023).

2. *Чернышенко: почти 50 тыс. кибератак отразили в РФ в 2022 году*. URL: https://www.interfax-russia.ru/main/churnyshenko-pochti-50-tys-kiberatak-otrazili-v-rf-v-2022-godu (дата обращения: 25.12.2023).

3. *Центр по компьютерным инцидентам фиксирует более 170 кибератак на РФ ежедневно*. URL: https://www.interfax.ru/digital/903202 (дата обращения: 25.12.2023).

4. *ТВ-инциденты вики — Энциклопедия инцидентов на ТВ*. URL: https://tv-incidents.fandom.com/ru/wiki/ (дата обращения: 25.12.2023).

5. *Указ Президента Российской Федерации «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»*. URL: http://publication.pravo.gov.ru/Document/View/0001202203300001 (дата обращения: 25.12.2023)

Об авторах:

Николай Николаевич Чибинев, кандидат технических наук, доцент кафедры экологии и промышленной безопасности Южно-Российского государственного политехнического университета (НПИ) (346428, РФ, г. Новочеркасск, ул. Просвещения, 132), fire.expert.ug@gmail.com

Станислав Ростиславович Федосеев, студент Южно-Российского государственного политехнического университета (НПИ) (346428, РФ, г. Новочеркасск, ул. Просвещения, 132), kineskopi_best@vk.com

Александр Николаевич Павлов, студент Южно-Российского государственного политехнического университета (НПИ) (346428, РФ, г. Новочеркасск, ул. Просвещения, 132), pavlovb123904@gmail.com

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Nikolai N. Chibinev, Cand. Sci. (Eng.), Associate Professor of the Ecology and Industrial Safety Department, Platov South-Russian State Polytechnic University (NPI) (132, Prosveshcheniya Str., Novocherkassk, 346428, RF), fire.expert.ug@gmail.com

Stanislav R. Fedoseev, Student, Platov South-Russian State Polytechnic University (NPI) (132, Prosveshcheniya Str., Novocherkassk, 346428, RF), kineskopi_best@vk.com

Aleksandr N. Pavlov, Student, Platov South-Russian State Polytechnic University (NPI) (132, Prosveshcheniya Str., Novocherkassk, 346428, RF), pavlovb123904@gmail.com

Conflict of interest statement: the authors do not have any conflict of interest.

All authors have read and approved the final manuscript.