Фемида.Science / Femida.Science. 2025;(2):150-156

Экономика / Economy

Научная статья
УДК 338.342.44
EDN: QYMBJN

Предупреждение киберпреступлений в условиях цифровой трансформации

Марина Сергеевна Шавишева

Российский государственный университет правосудия имени В. М. Лебедева, Москва, Российская Федерация
✉ *mshavisheva05@mail.ru*

Научный руководитель: **Е. Е. Макарова**, к.э.н., доцент, доцент кафедры экономики Российского государственного университета правосудия имени В. М. Лебедева

Аннотация. В статье рассматриваются современные подходы для применения технологий, которые обезвреживают киберпреступления. В условиях растущей угрозы кибератак, быстро набирающей темп цифровизации общества исследование направлено на установление и анализ эффективных инструментов, которые используются для обнаружения и предотвращения киберпреступлений. Цель статьи – изучить и исследовать методы защиты данных, проанализировать поведение компьютерной системы под воздействием информационных угроз на примере государственной корпорации «Ростех» и ПАО «Газпром». Результаты исследования могут быть полезны для специалистов в области информационной безопасности.

Ключевые слова: киберугрозы, кибератаки, информационная безопасность, атака, анализ, технологии, организация, киберпреступление

Для цитирования: Шавишева М. С. Предупреждение киберпреступлений в условиях цифровой трансформации // Фемида.Science. 2025. № 2 (17). С. 150–156.

Original article

Cybercrime Prevention in the Context of Digital Transformation

Marina S. Shavisheva

Russian State University of Justice named after V. M. Lebedev,
Moscow, Russian Federation
✉ *mshavisheva05@mail.ru*

Scientific supervisor: **E. E. Makarova**, Candidate of Science (Economic), Associate Professor, Associate Professor at the Economics Department of the Russian State University of Justice named after V. M. Lebedev

Abstract. The article discusses modern approaches to the application of technologies that neutralize cybercrime. In the context of the growing threat of cyber-attacks and the rapidly accelerating pace of digitalization of society, the study aims to review and analyze effective tools that are used to detect and prevent cybercrimes. The purpose of the article is to study and investigate data protection methods, to analyze the behavior of a computer system under the influence of information threats using the example of the Rostec State Corporation and Gazprom PJSC. The results of the study may be useful for information security specialists.

Keywords: cyber threats, cyber-attacks, information security, attack, analysis, technology, organization, cybercrime

For citation: Shavisheva, M. S. Cybercrime prevention in the context of digital transformation. *Femida.Science = Themis.Science.* 2025;(2):150-156. (In Russ.)

В настоящее время в условиях растущей цифровизации общества наблюдается ежегодное увеличение числа киберпреступлений (рис. 1), что требует симметричного ответа в виде разработки и внедрения новых подходов к их предотвращению. В 2024 г. количество киберпреступлений достигло своего пика – 765,4 тыс. Это на 13% больше, чем за этот же период 2023 г.[1]

Внедрение современных информационных технологий в производственный процесс предусматривает возможность максимально повысить эффективность и качество как самой производственной деятельности, так и выпускаемой продукции (услуг) [1]. Системы информационной безопасности должны включать подходы инновационного обнаружения новых сложных систем, которые способствуют развитию продвинутых технологий и решению новых угроз и задач [2].

Для минимизации числа киберпреступлений необходимо исследование цифровых технологий и правильное их применение организациями и пред-

[1] Число киберпреступлений в России // Tadviser. Государство, бизнес, технологии : [сайт]. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 19.02.2025).

приятиями. Ввиду значимости исследуемой категории необходимо провести изучение критериев и индикаторов обеспечения финансовой безопасности Российской Федерации, что будет способствовать своевременному выявлению проблем в этой сфере [4].

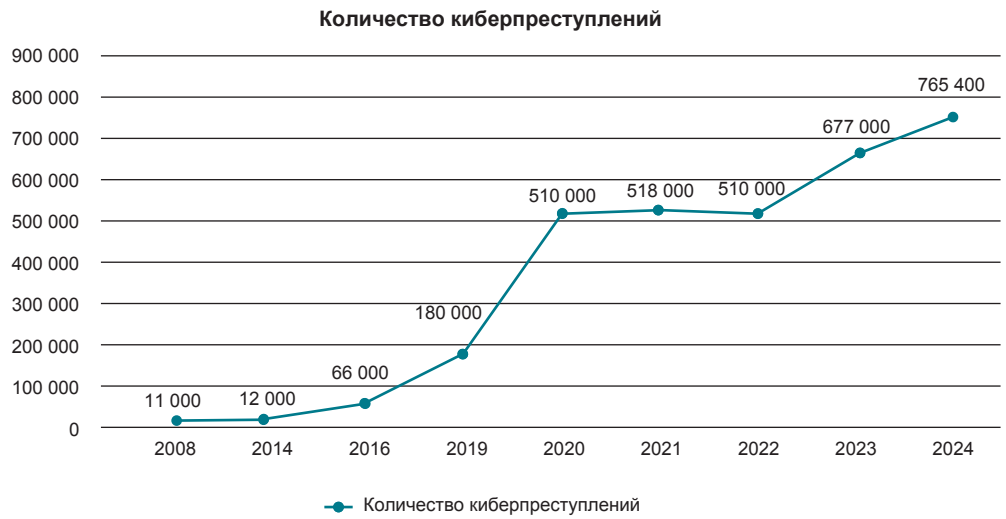

Рис. 1. График роста числа киберпреступлений с 2008 по 2024 г.[2]

Цель применения цифровых технологий для обезвреживания киберпреступлений – защита физических и юридических лиц, а также государства от мошенников, утечки конфиденциальных данных, финансовых потерь, использования пиратского контента и т. п. В задачи входят также разработка правовых и технических мер противодействия таким правонарушениям и создание специальных подразделений для их расследования.

Рассмотрим пример применения информационных технологий для защиты данных и предотвращения кибератак на примере Государственной корпорации «Ростех» (далее – «Ростех»)[3].

«Ростех» – это российская государственная корпорация, созданная в конце 2007 г. для помощи и содействия в разработке и производстве высокотехнологичной промышленной продукции, которая предназначена для гражданского и военного назначения[4].

---

[2] Составлен автором по данным анализа: Число киберпреступлений в России (см. сноску 1); [3].

[3] Ростех представил на ЦИПР систему противодействия кибератакам // Ростехнадзор : [сайт]. URL: https://www.gosnadzor.ru/news/67/8505/ (дата обращения: 17.02.2025).

[4] Россия: географические факторы и природные богатства ЦФО : метод. пособие для вузов / авт.-сост. В. М. Марасанова. Ярославль : ИПК «Индиго», 2023. 80 с. URL: https://www.uniyar.ac.ru/upload/medialibrary/f20/1_Rossia_geograficheskie_faktory.pdf.

Компания «РТ-информационная безопасность», которая входит в корпорацию «Ростех», представила на форуме «Цифровая индустрия промышленной России» (ЦИПР) отечественную систему RT Protect EDR для обнаружения кибератак и противодействия им. Кроме того, в настоящее время активно ведет работу центр SOC (отдел компании, который занимается постоянным отслеживанием состояния IT-инфраструктуры и защитой от киберугроз). В нем используются современные практики и технологии, которые представлены на рис. 2.

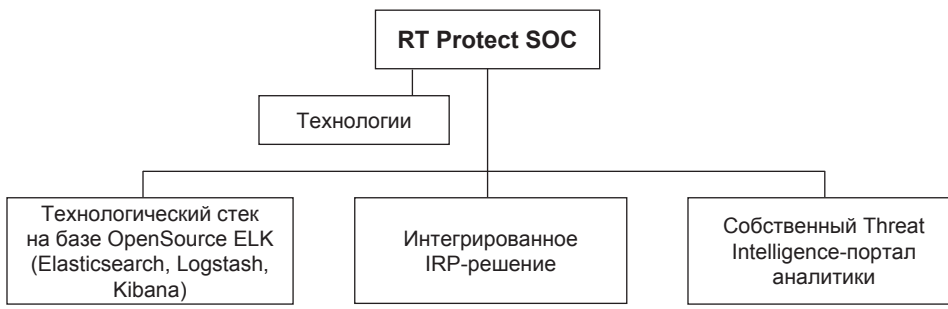

Рис. 2. Технологии SOC Ростех[5]

Рассматривая технологии SOC Ростех, необходимо выделить следующие.

1. ELK-стек – это технологический стек на базе опенсорс-проектов Elasticsearch, Logstash и Kibana. Он позволяет быстро и безопасно извлекать данные в нужном формате из любых источников и работать с этой информацией, осуществляя поиск, анализ или визуализацию в режиме реального времени.

• Elasticsearch – хранилище для быстрого и эффективного поиска, а также анализа больших объемов данных. Оно сочетает в себе различные функции базы данных, поисковой и аналитической системы.

• Logstash – приложение для сбора информации из всех возможных источников, преобразования ее в удобный для работы формат. Logstash позволяет фильтровать, массировать и структурировать интересующие данные.

• Kibana – небольшое дополнение для Elasticsearch, которое отвечает за визуализацию данных, аналитику и представление итоговой информации в удобном для восприятия виде. Kibana позволяет быстро анализировать итоги поиска, выискивать закономерности и представлять, где именно в проекте находятся недоработанные и слабые места.

2. Интегрированное IRP-решение. Интегрированное IRP-решение в RT Protect SOC Государственной корпорации «Ростех» позволяет уменьшить время реагирования на инцидент до 5 минут.

3. Собственный Threat Intelligence-портал аналитики позволяет загружать файлы для анализа и интегрирован с VirusTotal – это онлайн-плат-

[5] Составлено автором по данным анализа: РТ-Информационная безопасность. URL: https://rt-ib.ru/docs.html (дата обращения: 17.02.2025).

форма, предназначенная для проверки файлов и веб-ресурсов на вирусы и другое вредоносное программное обеспечение. Портал предоставляет актуальную подробную информацию об угрозах по CVE, IP-адресам, хэшам, доменам, URL, правилам, техникам и тактикам, данным WHOIS и другим параметрам.

Рассмотрим также использование современных практик и технологий для обезвреживания киберпреступлений ПАО «Газпром» (рис. 3), российской энергетической компании, более 50% акций которой контролирует государство. Основные направления ее работы – геологоразведка, добыча, транспортировка, хранение, переработка и реализация газа, газового конденсата и нефти. Она занимается в том числе производством и сбытом электроэнергии.

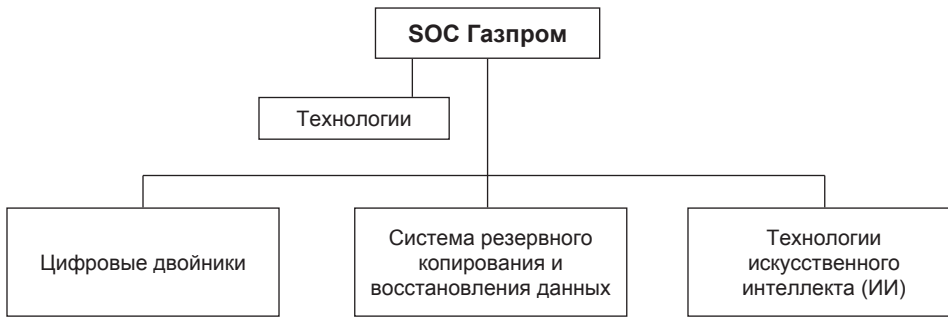

Рис. 3. Технологии SOC Газпром[6]

1. Цифровые двойники – это виртуальные копии объектов, которые имеют физические характеристики и сопровождаются процессами внутри объекта. Главным процессом цифровых двойников является обеспечение кибербезопасности объекта и прогноз работы оригинала в различных условиях. Также цифровые двойники при обнаружении атаки помогают реальному объекту незамедлительно начать расследование.

2. Система резервного копирования и восстановления данных осуществляется на базе «Кибер Бэкап»[7]. Российская база «Кибер Бэкап» специализируется на восстановлении и копировании данных от различных вирусов. Ее используют как ПАО «Газпром», так и большинство его дочерних компаний, например ООО «Газпром трансгаз Сургут».

3. Технологии искусственного интеллекта (ИИ) способствуют:

• обнаружению угроз, установлению возможных угроз;

• прогнозированию и предотвращению будущих атак на основе анализа произошедших вторжений;

---

[6] Составлено автором по данным анализа: Информационная безопасность ОАО «Газпром»: проблемы гиганта // Информационная безопасность : [сайт]. URL: https://lib.itsec.ru/articles2/focus/informacionaya_bezopasnost_oao (дата обращения: 16.02.2025).

[7] Как «Кибер Бэкап» защищает данные бизнеса // ixbt.com : [сайт]. URL: https://www.ixbt.com/infopages/cyber-backup.html (дата обращения: 19.02.2025).

• анализированию информации о пользователе и блокированию подозрительных действий.

Цифровая трансформация требует высококвалифицированных специалистов, способных работать с новыми технологиями, такими как искусственный интеллект, интернет вещей (IoT), робототехника и аналитика больших данных [5].

В результате анализа систем информационной безопасности, используемых в деятельности Госкорпорации «Ростех» и ПАО «Газпром», было выявлено, что у каждой крупной организации есть возможности и свои пути предотвращения кибератак. Данные технологии эффективно применяются на практике, при этом у них есть существенные отличия, эффективные для каждой организации в отдельности.

Несмотря на это, при обнаружении киберугрозы разные организации предпринимают шаблонные меры:

1) минимизация ущерба с помощью изоляции. Чтобы избежать заражения сети при обнаружении кибератаки, необходимо быстро ее изолировать;

2) своевременный анализ и Incident Response. Сотрудники должны своевременно проводить анализ угроз, устанавливать их источник и реагировать на инциденты;

3) принятие мер по устранению уязвимостей. Необходимо предпринимать меры по предотвращению повторного возникновения атак и угроз с помощью выявления уязвимостей в сетях;

4) быстрое восстановление систем и работоспособности данных в случае их повреждения;

5) полный анализ инцидента с выявлением причин угроз для составления шаблонного метода недопущения подобных инцидентов в будущем.

В соответствии с данным шаблоном описываются подробные инструкции и процедуры Play-book, которые необходимо предпринять при обнаружении информационных угроз.

Быстрое развитие технологий требует постоянного обновления знаний и навыков специалистов, а также адаптации существующих систем защиты к новым угрозам. Кроме того, необходимо учитывать аспекты правового регулирования и этические вопросы, связанные с использованием цифровых технологий.

В заключение можно признать, что меры предотвращения кибератак достаточно эффективны. У каждой организации они свои, и каждая компания применяет свои технологии. Однако у всех очень похожий алгоритм действий при появлении угрозы извне.

Список источников

1. Милкина Ю. А., Макарова Е. Е. Внедрение современных информационных технологий в строительную отрасль // Организатор производства. 2021. Т. 29, № 3. С. 101–110.

2. Сыщикова Е. Н., Макарова Е. Е., Муратова М. Н. Обоснование необходимости внедрения непрерывного процесса обеспечения информационной безопасности на предприятиях // Наука Красноярья: экономический журнал. 2024. Т. 13, № 1. С. 7–21.

3. Шавишева М. С. Анализ поведения компьютерной системы под воздействием информационных угроз // Инновационное развитие экономики России: вызовы и решения : материалы VI Всерос. науч.-практ. конф. (Москва, 17 апреля 2024 г.) / сост. Н. А. Ершова, О. В. Юткина. М. : РГУП, 2024. С. 68–73.

4. Александрова М. В., Проскурина З. Б., Юткина О. В. Влияние политики государства на финансовую безопасность страны в условиях цифровизации // Управленческий учет. 2024. № 9. С. 450–455.

5. Сыщикова Е. Н., Макарова Е. Е. Конвергентные проблемы управления инновационно-промышленным развитием экономических систем на современном этапе // Организатор производства. 2024. Т. 32, № 3. С. 53–65.

References

1. Milkina, Yu. A., Makarova, E. E. Introduction of modern information technologies in the construction industry. *Organizer of Production.* 2021;29(3):101-110. (In Russ.)

2. Syshchikova, E. N., Makarova, E. E., Muratova, M. N. Substantiation of the need to implement a continuous information security process at enterprises. *Krasnoyarsk Science: Economic Journal.* 2024;13(1):7-21. (In Russ.)

3. Shavisheva, M. S. Analysis of the behavior of a computer system under the influence of information threats. In: N. A. Ershova, O. V. Yutkina, comp. *Innovative development of the Russian economy: challenges and solutions.* Materials of the VI All-Russian Scientific and Practical Conference (Moscow, 17 April 2024). Moscow: Russian State University of Justice; 2024. Pp. 68–73. (In Russ.)

4. Alexandrova, M. V., Proskurina, Z. B., Yutkina, O. V. The influence of state policy on the financial security of the country in the conditions of digitalization. *Upravlencheskij uchet = Management Accounting*. 2024:(9):450-455. (In Russ.)

5. Syshchikova, E. N., Makarova, E. E. Convergent problems of management of innovation-industrial development of economic systems at the present stage. *Organizer of Production*. 2024;32(3):53-65. (In Russ.)

Информация об авторе

М. С. Шавишева – студент 3 курса.

Information about the author

M. S. Shavisheva – 3rd year student.

Автор заявляет об отсутствии конфликта интересов.

The author declares no conflict of interests.

Статья поступила в редакцию 04.03.2025; одобрена после рецензирования 13.03.2025; принята к публикации 05.05.2025.

The article was submitted 04.03.2025; approved after reviewing 13.03.2025; accepted for publication 05.05.2025.