www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.2.6

УДК 004.775:004.056
ББК 32.972.53

ОЦЕНКА РИСКОВ И УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ В ИНФОРМАЦИОННЫХ СИСТЕМАХ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Руслан Берикович Сеналиев

Магистрант, кафедра информационной безопасности,
Волгоградский государственный университет
Senalievruslan01@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Владислав Георгиевич Яриков

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
yarikov.vladislav@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье анализируются основные подходы к оценке рисков и управлению безопасностью информационных систем в секторе критической инфраструктуры. Обсуждаются методы оценки рисков, стратегии обеспечения безопасности, а также планирование действий на случай инцидентов. Отдельное внимание уделено законодательным аспектам и стандартам, как международным, так и специфическим для России, а также актуальным технологическим трендам и будущему развитию в области защиты критической инфраструктуры.

Ключевые слова: оценка рисков, управление безопасностью, критическая инфраструктура, информационные системы, новые технологии, киберугрозы.

В современном мире, где технологии играют критически важную роль в поддержании основных функций общества, информационные системы критической инфраструктуры становятся ключевыми элементами национальной и глобальной безопасности. Эти системы, включая энергетику, транспорт, здравоохранение и финансовые службы, обеспечивают жизненно необходимые услуги, поддерживающие социальную стабильность и экономическое процветание. Однако с ростом зависимости от цифровых технологий возрастает и уровень уязвимости перед лицом киберугроз, что делает оценку рисков и управление безопасностью критически важными процессами для обеспечения непрерывности и надежности этих жизненно важных функций.

Проблематика безопасности информационных систем критической инфраструктуры охватывает широкий спектр вызовов, включая защиту от кибератак, обеспечение целостности данных и доступности услуг в условиях постоянно меняющихся угроз. В связи с этим оценка рисков становится не только инструментом предвидения потенциальных уязвимостей, но и основой для разработки комп-

лексных стратегий управления безопасностью, направленных на минимизацию возможных последствий инцидентов.

Критическая инфраструктура охватывает системы и активы, жизненно необходимые для функционирования общества и экономики. Это включает в себя широкий спектр секторов, таких как энергетика, транспорт, здравоохранение, водоснабжение, телекоммуникации, финансы, правительственные услуги, а также производство и промышленность (см. рисунок). Каждый из этих секторов включает в себя определенные компоненты, такие как объекты инфраструктуры, сети связи, базы данных и информационные системы, которые обеспечивают их функционирование [4]. Важность этих компонентов подчеркивается их ролью в обеспечении непрерывности критически важных услуг и поддержании жизненного уровня населения.

В контексте информационной безопасности критическая инфраструктура сталкивается с множеством угроз, которые могут исходить как из внешних, так и из внутренних источников [2]. К внешним угрозам относятся кибератаки, направленные на нарушение функционирования инфраструктурных объектов или кражу чувствительной информации. Внутренние угрозы могут включать в себя технические сбои, ошибки в программном обеспечении и человеческий фактор, в результате которых также может быть нарушена работа критической инфраструктуры. Основные вызовы безопасности, с которыми сталкивается критическая инфраструктура, представлены в таблице.

Управление данными угрозами и вызовами требует комплексного подхода, включающего в себя не только технические средства защиты, но и разработку нормативно-правовой базы, обучение персонала и создание системы оперативного реагирования на инциденты безопасности.

Оценка рисков является ключевым элементом процесса управления безопасностью в критических инфраструктурах. Этот процесс включает в себя идентификацию потенциальных угроз, анализ уязвимостей, оценку вероятности наступления событий и определение их потенциального воздействия на функционирование инфраструктуры. Основные методологии оценки рисков могут включать каче-

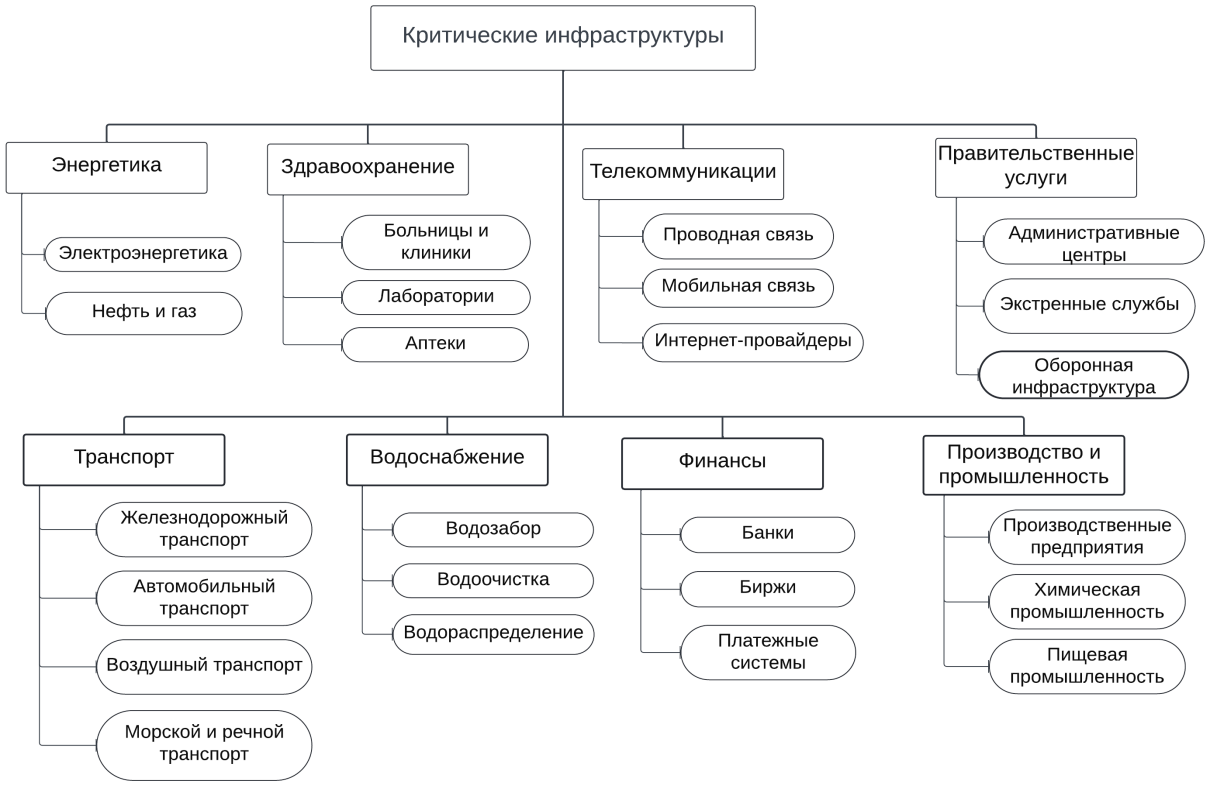

Схема критических инфраструктур

ственный, количественный и смешанный анализ [7].

Качественный анализ оценивает угрозы и уязвимости на основе экспертных мнений и исторических данных для определения уровней риска как «низкий», «средний» или «высокий».

Количественный анализ стремится присвоить числовые значения вероятности и последствиям угроз, используя статистические данные и математическое моделирование.

Смешанный анализ сочетает в себе элементы обоих подходов для достижения баланса между точностью и практичностью.

На основе оценки рисков разрабатываются стратегии управления, включающие предотвращение, снижение, перенос и принятие риска. Эти стратегии направлены на минимизацию вероятности наступления нежелательных событий и смягчение их последствий.

Разработка плана реагирования на инциденты является критически важным компонентом управления безопасностью. Этот план должен включать процедуры идентификации, оценки, реагирования и восстановления после инцидентов безопасности [8]. Основные элементы плана включают:

– **идентификация инцидентов:** механизмы и инструменты для обнаружения нарушений безопасности в реальном времени;

– **оценка инцидентов:** процедуры для определения масштаба, серьезности и потенциального воздействия инцидента;

– **реагирование на инциденты:** четкие инструкции по принятию мер, направленных на ограничение ущерба, изоляцию угрозы и восстановление нормального функционирования систем;

– **восстановление после инцидентов:** планы по восстановлению операций и минимизации простоев, а также процедуры для анализа инцидентов с целью извлечения уроков и улучшения будущей устойчивости.

Эффективное управление безопасностью требует непрерывной оценки рисков и адаптации планов реагирования на инциденты в соответствии с меняющимся ландшафтом угроз и развитием технологий.

Законодательное регулирование и стандарты играют фундаментальную роль в обеспечении безопасности критической инфраструктуры. Они устанавливают требования и руководящие принципы для организаций, относящихся к секторам критической инфраструктуры, помогая им формировать эффективные системы управления рисками и реагирования на инциденты. Ниже приведен обзор основных международных и национальных стандартов, а также законодательных актов, касающихся безопасности критической инфраструктуры.

ISO/IEC 27001. Международный стандарт, который определяет требования к системе менеджмента информационной безопасности (ISMS) для организаций любого типа и размера. Стандарт поддерживает защиту конфиденциальности, целостности и доступности информации путем применения рискового менеджмента [12].

NIST Cybersecurity Framework. Разработанный Национальным институтом стандартов и технологий США, этот фреймворк предоставляет набор индустриальных стандартов и лучших практик для управления и снижения киберсекьюрити рисков. Фреймворк поддерживает защиту критической инфраструктуры путем укрепления ее устойчивости к кибератакам [13].

GDPR (General Data Protection Regulation). Европейский регламент по защи-

Таблица

Вызовы безопасности критических инфраструктур

Вызов безопасности	Описание
Кибератаки	Использование вредоносного ПО, фишинг, DDoS-атаки и другие методы для нарушения работы объектов
Физическая безопасность	Защита объектов от несанкционированного доступа, саботажа и террористических актов
Зависимость от информационных технологий	Уязвимости в программном обеспечении и аппаратных средствах, которые могут быть использованы для нарушения работы систем
Человеческий фактор	Ошибки персонала, недостаточная квалификация или намеренные действия сотрудников, приводящие к нарушениям

те данных, устанавливающий правила защиты личных данных граждан Европейского Союза. Хотя GDPR прежде всего направлен на защиту данных, он также важен для критической инфраструктуры, поскольку включает требования по безопасности и уведомлению об инцидентах [14].

Директива ЕС о безопасности сетей и информационных систем (NIS Directive). Этот акт является первым законодательным актом ЕС, направленным на повышение уровня кибербезопасности во всех государствах-членах. Он устанавливает минимальные требования к безопасности и сообщения о серьезных инцидентах для операторов услуг ключевой значимости и провайдеров цифровых услуг [1].

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ. Принят в 2017 г., этот закон направлен на защиту критической информационной инфраструктуры от киберугроз. Он вводит понятие критической информационной инфраструктуры, устанавливает требования к ее защите, а также регулирует вопросы взаимодействия субъектов критической информационной инфраструктуры с государственными органами в сфере обеспечения безопасности [10].

Федеральный закон «О связи» № 126-ФЗ. Определяет правовые и организационные основы деятельности в области связи, включая вопросы безопасности и защиты информации в информационно-телекоммуникационных сетях, что непосредственно влияет на безопасность критических информационных инфраструктур [9].

Федеральный закон «О персональных данных» № 152-ФЗ. Устанавливает требования к обработке персональных данных, в том числе в части обеспечения их безопасности, что косвенно связано с защитой критической инфраструктуры, обрабатывающей такие данные [11].

Приказ ФСТЭК России от 25 декабря 2017 г. «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» № 239. Определяет механизмы реализации закона о безопасности критической информационной инфраструктуры, включая критерии отнесения объектов к критической информационной инфраструктуре и требования к их защите [6].

Эти и другие нормативно-правовые акты создают правовую основу для защиты критической инфраструктуры в Российской Федерации, определяя ответственность и обязанности субъектов критической инфраструктуры, а также устанавливая требования к обеспечению их безопасности от различных угроз.

В сфере обеспечения безопасности критической инфраструктуры намечается ряд ключевых тенденций, обусловленных быстрым развитием технологий и появлением новых угроз. Эти тенденции значительно влияют на методы и подходы к управлению безопасностью, предоставляя новые возможности для защиты критически важных активов и услуг. Ниже представлены некоторые из наиболее значимых технологических инноваций и направлений развития в этой области.

Искусственный интеллект и машинное обучение: ИИ и машинное обучение предлагают передовые способы обнаружения и предотвращения кибератак, а также автоматизации процессов мониторинга безопасности. Они могут анализировать большие объемы данных для выявления скрытых угроз и аномалий в поведении систем, что позволяет предпринимать проактивные меры защиты [3].

Блокчейн: технология блокчейн обеспечивает повышенную защиту данных благодаря своей децентрализованной и немодифицируемой природе. Применение блокчейна в защите критической инфраструктуры может помочь в обеспечении целостности и подотчетности данных, а также в защите от мошенничества и тамперинга.

Интернет вещей (IoT): расширение экосистемы IoT увеличивает сложность сетей критической инфраструктуры, внося новые вызовы в обеспечение безопасности. В то же время, развитие решений для безопасности IoT способствует более тесной интеграции и автоматизации процессов управления безопасностью в физическом и цифровом мирах.

Квантовые технологии: развитие квантовых вычислений обещает радикальные

изменения в области криптографии и защиты данных. Квантовые алгоритмы могут как создавать новые угрозы для существующих методов шифрования, так и предлагать новые, квантово-устойчивые решения для защиты информации [5].

Регулятивные технологии (RegTech): разработка и внедрение регулятивных технологий помогают организациям соблюдать законодательные и нормативные требования в области безопасности, автоматизируя сбор данных и отчетность, что способствует повышению прозрачности и управления рисками.

Прогресс в этих и других направлениях технологического развития предлагает значительные перспективы для усиления безопасности критической инфраструктуры. Однако он также требует от организаций гибкости в адаптации к новым угрозам и вызовам, а также постоянного обновления знаний и компетенций в области кибербезопасности.

Обеспечение безопасности критической инфраструктуры в современном цифровом мире является приоритетной задачей, требующей комплексного подхода и постоянной адаптации к меняющимся условиям. Важность проактивной оценки рисков и разработки стратегий управления безопасностью не может быть переоценена, поскольку они обеспечивают надежность и стабильность жизненно важных функций общества.

Законодательное регулирование и стандарты служат основой для защиты, однако эффективность их применения зависит от способности к инновациям и сотрудничеству на всех уровнях – от национального до международного. Внедрение новых технологий предлагает значительные перспективы для улучшения безопасности, но также влечет за собой новые вызовы.

В будущем ключом к защите критической инфраструктуры станут инновации, обмен знаниями и глубокое понимание угроз. Непрерывное совершенствование, координированные усилия государства, бизнеса и международного сообщества, а также адаптация к новым реалиям и технологиям будут определять успех в обеспечении безопасности на долгосрочную перспективу.

СПИСОК ЛИТЕРАТУРЫ

1. В ЕС приняли новую директиву по обеспечению высокого уровня кибербезопасности // Интерфакс: новости. – Электрон. текстовые дан. – Режим доступа: https://www.interfax.ru/world/874554

2. Ватрушкин, А. А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации / А. А. Ватрушкин // Евразийская адвокатура. – 2017. – № 6 (31). – С. 78–84.

3. Ерохин, С. Д. Управление безопасностью критических информационных инфраструктур / С. Д. Ерохин, А. Н. Петухов, П. Л. Пилюгин. – М. : Горячая линия – Телеком, 2024. – 240 с.

4. Карасёв, П. А. Кибербезопасность критически важной инфраструктуры: новые вызовы / П. А. Карасёв, Д. В. Стефанович // Россия в глобальной политике. – 2022. – № 6 (20). – С. 147–164. – DOI: 10.31278/1810-6439-2022-20-6-147-164

5. Карпов, М. А. Методика управления системой информационной безопасности объекта критической инфраструктуры / М. А. Карпов // Известия Тульского государственного университета. Технические науки. – 2021. – № 12. – С. 235–246. – DOI: 10.24412/2071-6168-2021-12-235-247

6. Приказ ФСТЭК РФ от 25.12.2017 № 239 – Редакция от 20.02.2020 // Контур.Норматив. – Электрон. текстовые дан. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=449296

7. Системы классификации и оценки уязвимостей и угроз информационных систем: какие они бывают и зачем нужны // Хабр. – Электрон. текстовые дан. – Режим доступа: https://habr.com/ru/companies/bastion/articles/706884/

8. Управление рисками информационной безопасности. Часть 1. Основные понятия и методология оценки рисков // Security Vision. – Электрон. текстовые дан. – Режим доступа: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-1-osnovnye-ponyatiya-i-metodologiya-otsenki-ri/

9. Федеральный закон от 07.07.2003 № 126-ФЗ – Редакция от 06.04.2024 // Контур.Норматив. – Электрон. текстовые дан. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=468989

10. Федеральный закон от 26.07.2017 № 187-ФЗ – Редакция от 10.07.2023 // Контур.Норматив. – Электрон. текстовые дан. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=453214

11. Федеральный закон от 27.07.2006 № 152-ФЗ – Редакция от 06.02.2023 // Контур.Норматив. – Электрон. текстовые дан. – Режим доступа: https://

normativ.kontur.ru/document?moduleId=1&documentId=447363&cwi=11006

12. ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) // Ассоциация по сертификации «Русский Регистр». – Электрон. текстовые дан. – Режим доступа: https://rusregister.ru/standards/iso-27001/

13. NIST Cybersecurity Framework // National Institute of Standards and Technology. – Electronic text data. – Mode of access: https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

14. The General Data Protection Regulation // Consilium. – Electronic text data. – Mode of access: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

REFERENCES

1. V ES prinjali novuju direktivu po obespecheniju vysokogo urovnja kiberbezopasnosti [The EU Adopted a New Directive to Ensure a High Level of Cyber Security]. *Interfaks: novosti* [Interfax: News]. URL: https://www.interfax.ru/world/874554

2. Vatrushkin A.A. Pravovye osnovy obespechenija kiberbezopasnosti kriticheskoj infrastruktury Rossijskoj Federacii [Legal Bases for Ensuring Cybersecurity of Critical Infrastructure of the Russian Federation]. *Evrazijskaja advokatura* [Eurasian Advocacy], 2017, no. 6 (31), pp. 78-84.

3. Erokhin S.D., Petukhov A.N., Pilyugin P.L. *Upravlenie bezopasnostyju kriticheskih informacionnyh infrastruktur* [Security Management of Critical Information Infrastructures]. Moscow, Goryachaya liniya – Telecom Publ., 2024. 240 p.

4. Karasyov P.A., Stefanovich D.V. Kiberbezopasnost kriticheski vazhnoi infrastruktury: novye vyzovy [Cyber Security of Critical Infrastructure: New Challenges]. *Rossija v globalnoj politike* [Russia in Global Politics], 2022, no. 6 (20), pp. 147-164. DOI: 10.31278/1810-6439-2022-20-6-147-164

5. Karpov M.A. Metodika upravlenija sistemoj informacionnoj bezopasnosti obyekta kriticheskoj infrastruktury [Methodology of Management of the Information Security System of the Critical Infrastructure Object]. *Izvestija Tulskogo gosudarstvennogo universiteta. Tehnicheskie nauki* [Izvestiya Tula State University. Technical Sciences], 2021, no. 12, pp. 235-246. DOI: 10.24412/2071-6168-2021-12-235-247

6. Prikaz FSTEK RF ot 25.12.2017 No. 239 – Redakcija ot 20.02.2020 [Order of the FSTEC of the Russian Federation of 25.12.2017 № 239 – Wording of 20.02.2020]. *Kontur.Normativ* [Contour.Normative]. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=449296

7. Sistemy klassifikacii i ocenki ujazvimostej i ugroz informacionnyh sistem: kakie oni byvajut i zachem nuzhny [Systems of Classification and Assessment of Vulnerabilities and Threats to Information Systems: What They Are and Why They Are Needed]. *Habr*. URL: https://habr.com/ru/companies/bastion/articles/706884/

8. Upravlenie riskami informacionnoj bezopasnosti. Chast 1. Osnovnye ponjatija i metodologija ocenki riskov [Information Security Risk Management. Part 1. Basic Concepts and Risk Assessment Methodology]. *Security Vision*. URL: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-1-osnovnye-ponyatiya-i-metodologiya-otsenki-ri/

9. Federalnyj zakon ot 07.07.2003 N 126-FZ – Redakcija ot 06.04.2024 [Federal Law of 07.07.2003 N 126-FZ – Wording of 06.04.2024]. *Kontur.Normativ* [Contour.Normative]. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=468989

10. Federalnyj zakon ot 26.07.2017 No. 187-FZ – Redakcija ot 10.07.2023 [Federal Law of 26.07.2017 N 187-FZ – Wording of 10.07.2023]. *Kontur.Normativ* [Contour.Normative]. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=453214

11. Federalnyj zakon ot 27.07.2006 No. 152-FZ – Redakcija ot 06.02.2023 [Federal Law of 27.07.2006 N 152-FZ – Wording of 06.02.2023]. *Kontur.Normativ* [Contour.Normative]. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=447363&cwi=11006

12. *ISO/IEC 27001 (GOST R ISO/MEK 27001)* [ISO/IEC 27001 (GOST R ISO/IEC 27001)]. *Associacija po sertifikacii «Russkij Registr»* [Certification Association "Russian Register"]. URL: https://rusregister.ru/standards/iso-27001/

13. NIST Cybersecurity Framework. *National Institute of Standards and Technology.* URL: https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

14. The General Data Protection Regulation. *Consilium*. URL: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

RISK ASSESSMENT AND SECURITY MANAGEMENT IN CRITICAL INFRASTRUCTURE INFORMATION SYSTEMS

Ruslan B. Senaliev

Master's Student, Department of Information Security,
Volgograd State University
Senalievruslan01@gmail.com
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy),
Associate Professor, Department of Information Security,
Volgograd State University
yarikov.vladislav@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article analyzes the main approaches to risk assessment and security management of information systems in the critical infrastructure sector. It discusses methods of risk assessment, security strategies, and planning for incident response. Special attention is given to legislative aspects and standards, both international and specific to Russia, as well as to current technological trends and future developments in the field of critical infrastructure protection. Ensuring the security of critical infrastructure in today's digital world is a priority task that requires a comprehensive approach and constant adaptation to changing conditions. The importance of proactive risk assessment and the development of security management strategies cannot be overemphasized, as they ensure the reliability and stability of vital societal functions. Legislation and standards provide the foundation for protection, but their effectiveness depends on the ability to innovate and collaborate at all levels, from national to international. The introduction of new technologies offers significant promise for improving security but also brings with it new challenges. In the future, the key to critical infrastructure protection will be innovation, knowledge sharing, and a deep understanding of threats. Continuous improvement, coordinated efforts by government, business, and the international community, and adaptation to new realities and technologies will determine long-term security success.

Key words: risk assessment, security management, critical infrastructure, information systems, new technologies, cyber threats.