Научная статья
УДК 004.7:630

СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ЦИФРОВОГО КОНТУРА ПРЕДПРИЯТИЙ ЛЕСНОЙ ОТРАСЛИ

Данил Сергеевич Ячменев[1], Евгений Николаевич Щепеткин[2]
[1, 2] Уральский государственный лесотехнический университет, Екатеринбург, Россия
[1] danilyachmenyov@outlook.com
[2] shchepetkinen@m.usfeu.ru

Аннотация. Рассмотрены угрозы кибербезопасности лесного комплекса. Предложена стратегия киберустойчивости, интегрирующая организационные, технические и образовательные меры для защиты цифрового контура.

Ключевые слова: киберустойчивость, лесной комплекс, информационная безопасность, цифровой контур

Для цитирования: Ячменев Д. С., Щепеткин Е. Н. Стратегия обеспечения киберустойчивости цифрового контура предприятий лесной отрасли // Научное творчество молодежи – лесному комплексу России = Scientific creativity of youth to the forest complex of Russia : материалы XXII Всероссийской (национальной) научно-технической конференции студентов и аспирантов. Екатеринбург : УГЛТУ, 2026. С. 1207−1210.

Original article

A STRATEGY FOR ENSURING CYBER RESILIENCE OF THE DIGITAL CONTOUR OF FOREST INDUSTRY ENTERPRISES

Danil S. Yachmenev[1], Evgeny N. Shchepetkin[2]
[1, 2] Ural State Forest Engineering University, Ekaterinburg, Russia
[1] danilyachmenyov@outlook.com
[2] shchepetkinen@m.usfeu.ru

Abstract. The potential threats to the cybersecurity of the forest sector are considered. A strategy for cyber resilience is proposed, which integrates organizational, technical, and educational measures to protect digital infrastructure.

Keywords: cyber resilience, forest complex, information security, digital contour

For citation: Yacmenev D. S., Shchepetkin E. N. (2026) Strategiya obespecheniya kiberustojchivosti cifrovogo kontura predpriyatij lesnoj otrasli [A strategy for ensuring cyber resilience of the digital contour of forest industry enterprises]. Nauchnoe tvorchestvo molodezhi – lesnomu kompleksu Rossii [Scientific crea-tivity of youth to the forest complex of Russia] : materials of the XXII All-Russian (national) Scientific and Technical Conference of undergraduate and postgraduate students. Ekaterinburg : USFEU, 2026. P. 1207–1210. (In Russ).

Современные предприятия лесного комплекса (ЛК) переживают этап активной цифровой трансформации. Внедрение систем точного лесоводства, спутникового мониторинга, беспилотных летательных аппаратов (БПЛА), интернета вещей (IoT) для отслеживания техники и SCADA-систем для управления технологическими процессами на лесопильных и целлюлозно-бумажных производствах формирует сложный цифровой контур. Данный контур становится критически важным активом, отказоустойчивость и безопасность которого напрямую влияют на экономическую и экологическую стабильность отрасли. Однако специфика ЛК делает его уязвимым для целевых кибератак, последствия которых могут варьироваться от хищения коммерческой информации до экологических катастроф и масштабных экономических потерь. В этом контексте традиционный подход, ориентированный лишь на предотвращение инцидентов, недостаточен. Требуется стратегия, нацеленная на обеспечение киберустойчивости – способности системы непрерывно выполнять свои функции перед лицом деструктивных кибервоздействий, адаптироваться к ним и восстанавливаться после них. Целью данной статьи является разработка комплексной стратегии обеспечения киберустойчивости цифрового контура предприятий лесной отрасли.

Цифровой контур ЛК характеризуется высокой степенью гетерогенности, объединяя операционные (OT) и информационные (IT) технологии. Ключевыми компонентами являются:

- геоинформационные системы (ГИС) и системы дистанционного зондирования Земли;
- системы управления предприятиями (ERP, CRM);
- автоматизированные системы управления технологическими процессами (АСУ ТП/SCADA) на перерабатывающих заводах;
- системы мониторинга транспорта и логистики на базе IoT;
- данные лесоустройства и кадастровые системы.

Специфические угрозы для данной экосистемы включают:

1) атаки на целостность и доступность геоданных: злоумышленное искажение данных о границах лесных участков, породном составе или данных дистанционного зондирования может привести к незаконным вырубкам, ошибкам в планировании и многомиллионным убыткам;

2) компрометация АСУ ТП: взлом систем управления на целлюлозно-бумажном комбинате или лесопильном заводе способен вызвать остановку производства, порчу оборудования или техногенную аварию [1];

3) кража интеллектуальной собственности: речь идет о планах лесовосстановления, запасах древесины, ноу-хау в области переработки, что подрывает конкурентные преимущества;

4) Ransomware-атаки: шифрование данных, парализующее работу предприятия, от планирования рубок до отгрузки готовой продукции;

5) цепочечные атаки через контрагентов: уязвимости в системах партнеров (логистических, сервисных компаний) могут быть использованы для проникновения в сеть головного предприятия.

Предлагаемая стратегия основывается на принципах проактивности, непрерывности и глубокой интеграции в бизнес-процессы. Она состоит из трех взаимосвязанных компонентов.

Организационно-управленческий компонент

На данном уровне осуществляется интеграция управления киберрисками в общую систему корпоративного управления:

- создание центра мониторинга безопасности (SOC): специализированный SOC для ЛК должен быть настроен на корреляцию событий не только из IT-сетей, но и из OT-сред (SCADA, IoT-сенсоры), а также внешних источников (данные спутникового мониторинга);
- внедрение системы управления рисками по стандартам (NIST CSF, ISO 27005): проведение регулярной оценки рисков с фокусом на критически важные активы – ГИС, АСУ ТП, базы данных лесоустройства. За основу может быть взят рамочный стандарт NIST CSF, обеспечивающий гибкий и комплексный подход [2];
- разработка и регулярное обновление плана реагирования на инциденты и обеспечения непрерывности бизнеса (IRP/BCP): План должен включать сценарии отработки атак на ключевые технологические процессы.

Технико-технологический компонент

Данный компонент нацелен на реализацию практических мер защиты:

- сегментирование сети: строгое разделение IT- и OT-сетей, а также сегментирование внутри OT-сегмента (например, отделение сети управления лесопилкой от сети управления котельной). Это является одной из базовых мер защиты критической информационной инфраструктуры [3];
- защита периметра и критических активов: внедрение межсетевых экранов нового поколения (NGFW), систем обнаружения и предотвращения вторжений (IDS/IPS), адаптированных для OT-протоколов;
- резервное копирование и восстановление: внедрение отказоустойчивой системы резервного копирования с регулярным тестированием процедур восстановления для ключевых данных (ГИС, конфигурации АСУ ТП).

Образовательно-просветительский компонент

Человеческий фактор остается одним из ключевых векторов атак. Требуется специализированное обучение персонала, которое включает проведение регулярных тренингов по кибергигиене не только для офисных сотрудников, но и для инженеров и технологов, работающих с АСУ ТП. Повышение осведомленности является ключевым элементом стратегии безопасности.

Модель реализации и ожидаемые результаты

Реализация стратегии должна носить итеративный характер по схеме «Оценка – Защита – Обнаружение – Реагирование – Восстановление». На первом этапе проводится аудит и картографирование цифрового контура. Затем внедряются базовые средства защиты и сегментации. Следующим шагом развертываются системы мониторинга и обнаружения аномалий. Завершающими циклами являются отработка механизмов реагирования и восстановления.

Ожидаемыми результатами внедрения стратегии являются:

- снижение времени простоя критических систем на 40…60 %.
- минимизация финансовых потерь от киберинцидентов;
- повышение доверия со стороны регуляторов, инвесторов и партнеров;
- создание конкурентного преимущества за счет надежности и предсказуемости бизнес-процессов.

Цифровая трансформация лесного комплекса необратима, а вместе с ней растет и киберугроза. Предложенная стратегия обеспечения киберустойчивости представляет собой комплексный ответ на этот вызов. Она позволяет перейти от пассивной защиты к построению адаптивной системы, способной противостоять современным кибератакам, минимизировать их последствия и обеспечивать непрерывное выполнение ключевых функций. Дальнейшие исследования целесообразно направить на разработку отраслевых стандартов и математических моделей для оценки уровня киберустойчивости конкретных предприятий лесного комплекса.

Список источников

1. Штефан Д. Защита промышленных систем управления: угрозы и меры противодействия // Труды СПИИРАН. 2020. Т. 19, № 2. С. 345–368.

2. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology (NIST), 2018. 55 p.

3. Соколов А. В., Петров И. И. Информационная безопасность объектов критической информационной инфраструктуры. М. : Горячая линия – Телеком, 2021. 254 с.