АНАЛИЗ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Шаров Илья Сергеевич
Главный специалист Отдела внедрения и обслуживания комплексных систем безопасности АО «Национальный Инновационный Центр»

Бутакова Наталья Георгиевна
кандидат физико-математических наук, доцент кафедр «Информационная безопасность» Московского политехнического университета и Национального исследовательского университета МИЭТ

Аннотация: *В данной статье изучена системность возникновения инцидентов информационной безопасности на субъектах КИИ и последствия их влияния. Отражен анализ применяемых промышленными предприятиями мер защиты инфраструктуры. Разработаны рекомендации по повышению защищенности АСУ ТП.*

Ключевые слова: *Цифровая экономика, Инцидент, Последствия, Безопасность, АСУ ТП, ДУСД, КИИ.*

Abstract: *This article presents a study that analyze informational security incidents, systematicity of it's occurrence on the subject of CII and it's consequences. It evaluates security measures of infrastructure used by industrial enterprises and proposes recommendations for strengthening protection of ICS/SCADA.*

Keywords: *Digital economy, Incident, Consequences, Security, ICS, SCADA, CII.*

Введение. Подготовка к четвертой промышленной революции трансформирует индустриальную инфраструктуру, повышает показатели эффективности с применением технологий цифровизации. Машинное обучение, анализ данных, робототехника, интернет вещей открывают огромные возможности технического и экономического прогресса для бизнеса и государств, но в тоже время это увеличивает количество векторов цифровых атак. Если до начала глобальной цифровизации промышленные предприятия были практически вне поля видимости киберпреступности, то в последние годы с применением информационных технологий нарушение безопасности автоматизированных систем управления технологическим процессом (далее АСУ ТП или ICS, – Industrial Control System), включающим в себя диспетчерское управление и сбор данных (далее ДУСД или SCADA, – Supervisory Control And Data Acquisition), стало обычным делом.

Применение разработок из области информационных технологий (далее IT, – Information Technology) в промышленности протекают нелегко, ведь ICS управляющие критически важными процессами в инфраструктуре энергетической, горнодобывающей, металлургической и химической и др. промышленности разрабатывались десятилетиями до привычных IT-сетей предприятий, со своими собственными протоколами. Цифровизация приводит к перестройке налаженных и стабильных процессов. Предприятия, руководствуясь желанием повысить производительность и снизить затраты, проводят внедрение цифровых технологий, несмотря на повышенный риск кибератак в следствие установления связи между IT и ICS. Преимущества очевидны: те предприятия, которые провели цифрорую трансформацию, получили почти в 2 раза больше прибыли [1], чем предприятия, которые не уделяют должного внимания цифровой экономике и следующей из нее цифровой трансформации.

Для киберпреступности АСУ ТП и ДУСД являются очень привлекательными целями. Предприятия в условиях цифровой экономики проводят автоматизацию своих бизнес-процессов и в погоне за прибылью упускают из виду процессы обеспечения информационной безопасности. Хакеры не упускают появляющихся возможностей и нарушают работоспособность предприятий с целью выкупа или атаки на критическую информационную инфраструктуру (далее КИИ) конкурентов и недружественных государств.

Рис.1 Субъекты КИИ, столкнувшиеся с системными инцидентами информационной безопасности

Цель исследования:

Изучить состояние защищенности автоматизированных систем управления технологическим процессом критической информационной инфраструктуры в условиях цифровой экономики.

Задачи исследования:

1. Исследовать системность возникновения инцидентов информационной безопасности вследствие эксплуатации уязвимостей на субъектах КИИ и последствия их влияния.
2. Проанализировать применяемые меры защиты инфраструктуры и используемые сетевые технологии.
3. Разработать рекомендации по повышению защищенности АСУ ТП.

Результаты проведенного международного опроса [2] лиц, ответственных за обеспечение информационной безопасности на 429 субъектах КИИ, показал, что практически 90% предприятий, применяющих ICS/SCADA, столкнулись с инцидентами информационной безопасности в своей инфраструктуре, и только 11% никогда не сталкивались с инцидентами информационной безопасности, что наглядно отображено на рисунке 1.

Многие промышленные предприятия применяют различные методы обеспечения информационной безопасности, но инциденты информационной безопасности в ICS/SCADA становятся обычным явлением и несут за собой существенный ущерб. В результате опроса [2] выяснилось, что вследствие инцидентов информационной безопасности на предприятиях, составляющих 63% от опрошенных, была сильно или критично затронута безопасность работавших сотрудников, 58% сообщили о значительном влиянии на финансовую стабильность предприятия, а 63% отметили серьезное снижение производительности, числовой эквивалент представлен на рисунке 2.

Несмотря на данные показатели, многие предприятия не применяли технологии и меры, направленные на повышение защищенности ICS/SCADA. При этом три четверти из них уже установили, как минимум, базовые связи между IT и ICS, что создало дополнительные угрозы эксплуатации существующих уязвимостей [3]. Такое развитие событий произошло в норвежской нефтегазовой и металлургической компании Norsk Hydro в марте 2019 года. Атака с использованием вредоносной программы LockerGoga вызвала остановку нескольких заводов и за первую неделю стоила компании 40 миллионов долларов США [3].

Специализированные вредоносные программы для атак на ICS/SCADA живут и выполняют свое предназначение достаточно долго после обнаружения и рассылки сигнатур, что подтверждают данные отчета [3], динамика обнаружения вредоносной программы вроде Industroyer за 2018

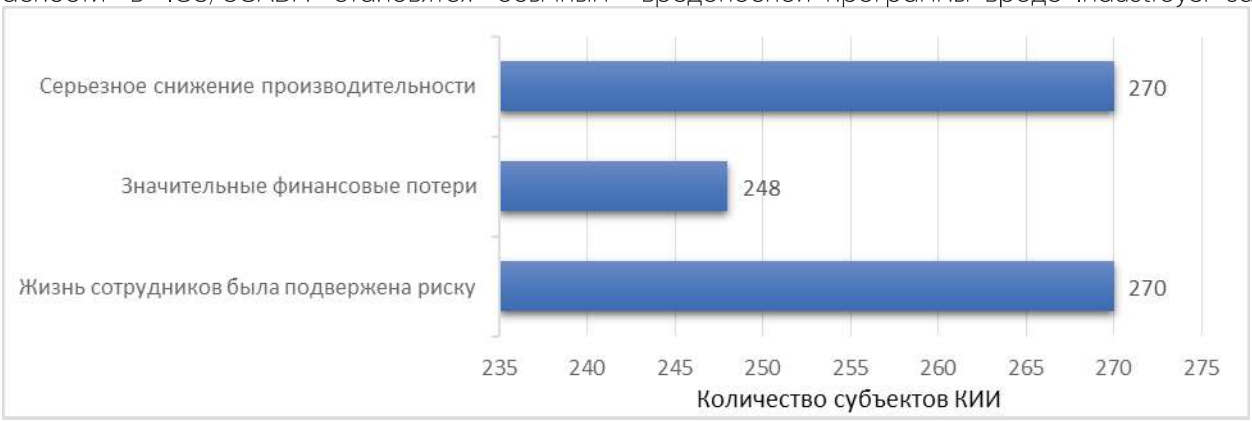

Рис.2 Последствия инцидентов информационной безопасности на субъектах КИИ

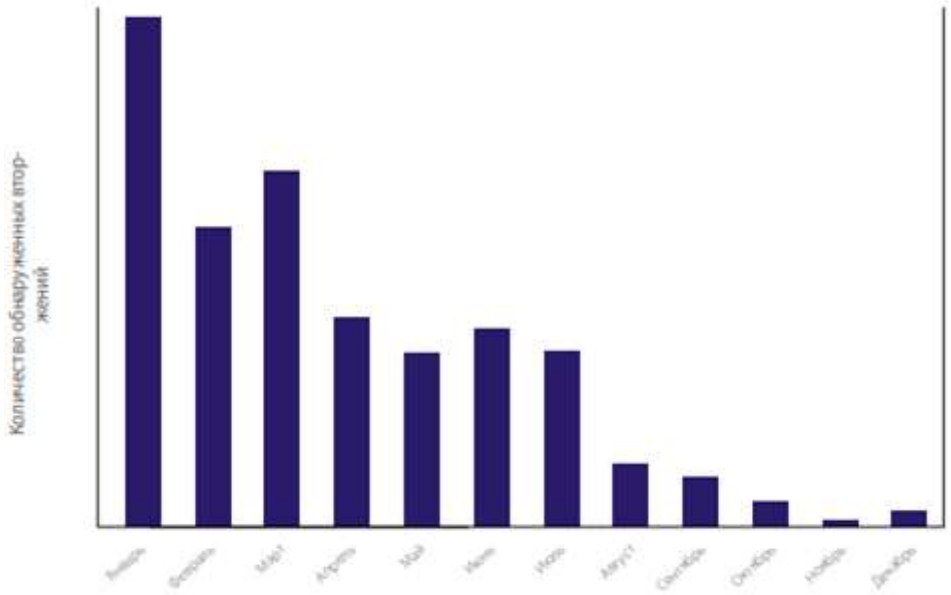

Рис.3 Частота обнаруженных вторжений вредоносной программы Industroyer[3]

год отображена на рисунке 3.

Только более половины предприятий применяют меры по обеспечению защиты конечных устройств, 50% опрошенных не использует шифрование трафика, 48% не используют систем контроля действий привилегированных пользователей и 42% не применяют ролевую модель разграничения доступа сотрудников, что наглядно изображено на рисунке 4.

Помимо этого, 64% предприятий предоставляют полные административные права поставщикам IT услуг для доступа к собственной инфраструктуре, 60% предоставляют полный или высокоуровневый административный доступ своим партнерам и более чем 50% предоставляют такой же уровень доступа для государственных органов [2]. Этот факт, несомненно, увеличивает риск несанкционированного доступа в системы управления технологическими процессами. Диаграмма предоставления административных прав изображена на рисунке 5

Предприятия в основном обеспокоены угрозой использования персональных устройств сотрудников, имеющих доступ к облачным технологиям, и возможностью реализации с помощью этих

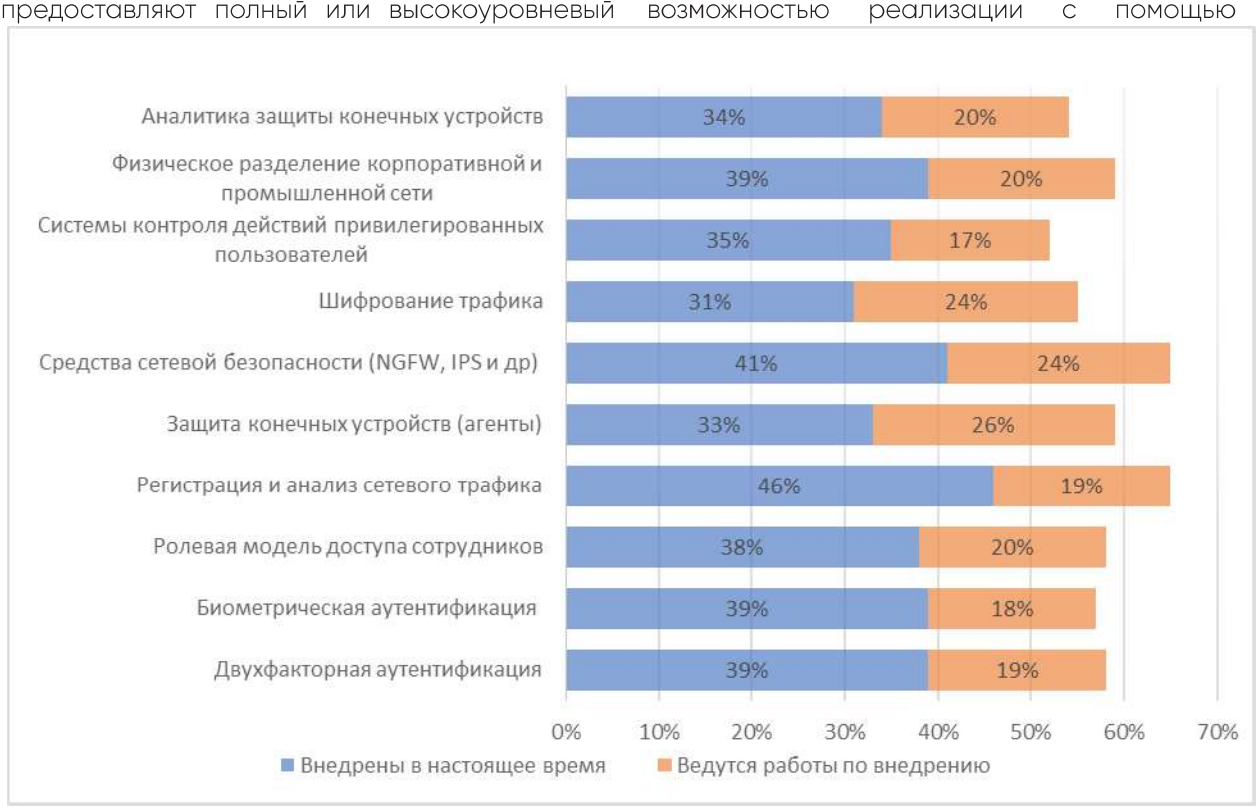

Рис.4 Применяемые меры защиты инфраструктуры [2]

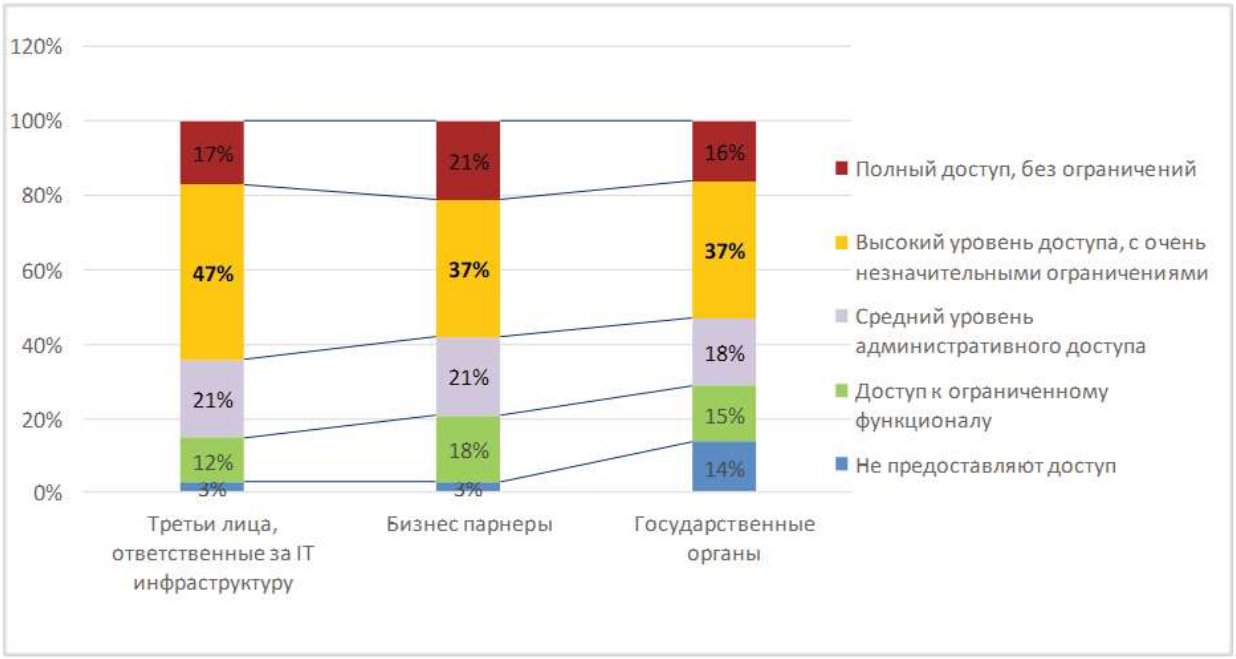

Рис.5 Предоставление административных прав третьей стороне

устройств несанкционированного доступа к ICS/SCADA. Примечательно, что каждое предприятие, принявшее участие в опросе, применяет технологии Интернета вещей или технологии беспроводной связи для подключения к своим сетям, в среднем приблизительно 5 технологий связанно с сетью предприятия, что отображено на рисунке 6. Такая ситуация также создает дополнительные риски несанкционированного вторжения и атак на АСУ ТП.

В качестве рекомендаций по повышению защищенности АСУ ТП на основе проведенного анализа применяемых мер защиты инфраструктуры и используемых сетевых технологий предлагаются следующие мероприятия:

- произвести сегментирование отдельных подключений к ICS/SCADA по технологическому признаку;
- организовать защиту сетевой инфраструктуры на всех уровнях иерархической модели (ядро сети, уровень распределения, уровень доступа);
- разработать и применить базовые политики по управлению правами доступа (предоставлению, разграничению, прекращению) для пользователей и администраторов инфраструктуры предприятия, а также регулирование предоставления прав доступа для третьей стороны;
- применить политики управления обновлениями ПО;
- использовать средства защиты веб-приложений (WAF);
- использовать системы защиты конечных устройств (EPR/EDR/ NGEPP);
- проводить анализ данных в режиме реального времени на наличие угроз (TDS).

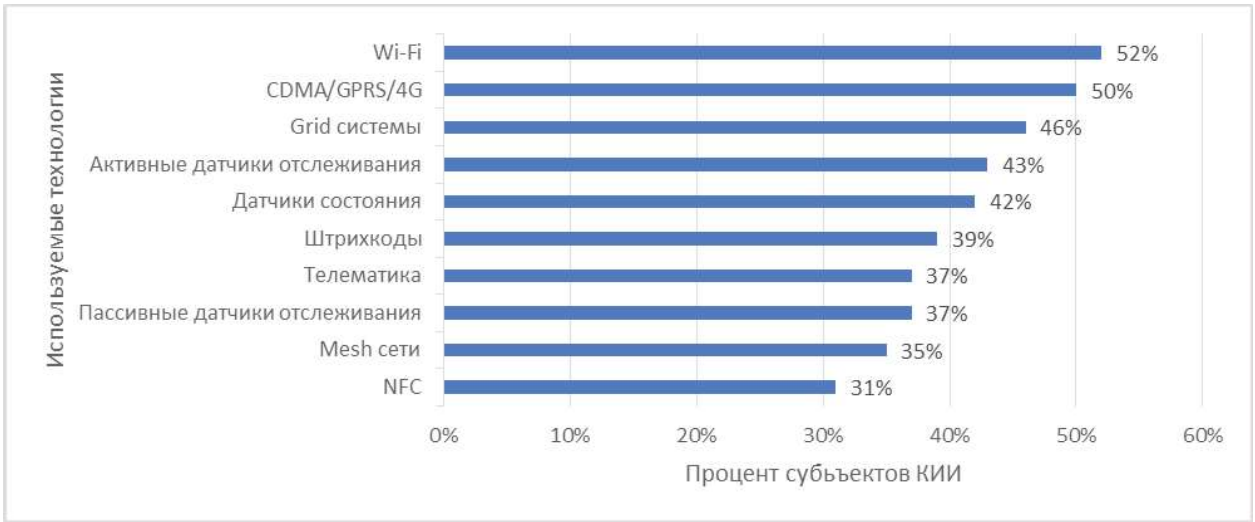

Рис.6 Технологии связанные с сетью ICS/SCADA [2]

Выводы:

1. Исследование инцидентов информационной безопасности показало, что их динамика усиливается, потому что многие предприятия не применяют современные технологии и меры, направленные на повышение защищенности ICS/SCADA даже после устранения последствий инцидентов и восстановления функционирования нарушенных процессов.
2. Проведенный анализ защищенности инфраструктуры КИИ выявил значительные упущения по совокупности применяемых мер защиты инфраструктуры. Отсутствует или применяется не в полной мере практика разграничения и предоставления прав доступа пользователям, в том числе администраторам и третьим лицам.
3. Понимание уязвимости сетевой инфраструктуры КИИ, ее сегментирование и защита, в совокупности с применением средств защиты конечных устройств и анализом трафика на наличие угроз в режиме реального времени должны быть взяты в качестве основы для повышения уровня защищенности предприятий. При этом необходимо применять базовые принципы менеджмента информационной безопасности.

Заключение

Цифровая экономика открывает перед предприятиями промышленности существенные преимущества, но при этом ICS/SCADA оказываются под прицелом современных и непрерывных угроз. Пропадает физическое разделение, которое ранее защищало данные системы от внимания хакеров и вредоносных программ.

Применяемые предприятиями меры обеспечения информационной безопасности недостаточны, это подтверждается динамикой системности возникновения инцидентов. В качестве основы для повышения уровня защищенности предприятий послужит понимание своей сетевой инфраструктуры, ее сегментирование и защита, в совокупности с применением средств защиты конечных устройств и анализ трафика на наличие угроз в режиме реального времени. При этом необходимо применять базовые принципы менеджмента информационной безопасности.

Защита ICS/SCADA должна отличаться от традиционных информационных систем, нарушение стабильно и бесперебойно выполняющихся процессов систем КИИ не только влияет на экономическую, социальную и политическую устойчивость региона или государства в целом, но и создает угрозу для жизней и здоровья людей.

Список литературы

1. Robert Bock, Marco Iansiti, Karim R. Lakhani, What the Companies on the Right Side of the Digital Business Divide Have in Common, Harvard Business Review, 2017 г [Электронный ресурс] – URL: https://hbr.org/2017/01/what-the-companies-on-the-right-side-of-the-digital-business-divide-have-in-common (дата обращения 01.12.19).
2. Fortinet Report Independent Study Pinpoints Significant SCADA/ICS Security Risks, June 2019 [Электронный ресурс] – URL: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Independent-Study-Pinpoints-Significant-Scada-ICS-Cybersecurity-Risks.pdf (дата обращения 06.12.2019)
3. Отчет лаборатории FortiGuards Labs, компании FortiNet о тенденциях в сфере безопасности операционных технологий за 2019 год – URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ru_ru/report-security-trends.pdf (дата обращения 20.12.19)