DOI 10.37882/2223–2966.2020.07.36

ПОВЫШЕНИЕ УРОВНЯ СТРАТЕГИЧЕСКОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

INCREASING THE LEVEL OF STRATEGIC SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

N. Fomin
A. Samoshina
O. Evsutin
N. Domukhovsky
D. Komarov

Summary. The article deals with increasing the level of strategic security of critical information infrastructure objects. Failure to operate such facilities can paralyze the life of cities and businesses, cause significant damage due to potential vulnerabilities and the inability to neutralize cyber threats. A comparative analysis of software and hardware complexes for ensuring the protection of critical information infrastructure is carried out. The list of shortcomings in existing software and hardware complexes is revealed, based on the specifics of the requirements for ensuring the security of objects of the Russian Federation. A list of proposals for improving software and hardware systems to ensure the protection of critical information infrastructure has been formed.

Keywords: cyber threats, automated process control systems, vulnerabilities, critical information infrastructure, strategic security.

Фомин Николай Александрович
Н.с., Институт проблем управления им. В. А. Трапезникова РАН, г. Москва
science-fomin@yandex.ru
Самошина Анна Ивановна
Инженер-исследователь, Институт проблем управления им. В. А. Трапезникова РАН, г. Москва
ania.cat03@gmail.com
Евсютин Олег Олегович
К.т.н., доцент, с.н.с., Институт проблем управления им. В. А. Трапезникова РАН, г. Москва
evsutin.oo@gmail.com
Домуховский Николай Анатольевич
Уральский центр систем безопасности, г. Екатеринбург
ndomukhovsky@ussc.ru
Комаров Денис Евгеньевич
Ведущий аналитик, Уральский центр систем безопасности, г. Екатеринбург
dkomarov@ussc.ru

Аннотация. В статье рассматривается повышение уровня стратегической безопасности объектов критической информационной инфраструктуры. Нарушение работоспособности подобных объектов способно парализовать жизнедеятельность городов и предприятий, нанести существенный урон за счет имеющихся потенциальных уязвимостей и невозможности нейтрализовать киберугрозы. Проведен сравнительный анализ программно-аппаратных комплексов обеспечения защиты критической информационной инфраструктуры. Выявлен перечень недостатков в существующих программно-аппаратных комплексах, исходя из специфики требований обеспечения безопасности объектов Российской Федерации. Сформирован перечень предложений по совершенствованию программно-аппаратных комплексов обеспечения защиты критической информационной инфраструктуры.

Ключевые слова: киберугрозы, АСУ ТП, уязвимости, КИИ, стратегическая безопасность.

Введение

В настоящее время существует необходимость обеспечения адекватного уровня информационной безопасности на критически важных объектах (КВО) и объектах критической информационной инфраструктуры (КИИ) Российской Федерации [1]. Для управления бизнес-процессами КВО и организаций, являющихся субъектами КИИ, используются АСУ ТП, выступающие основными элементами инфраструктуры современных предприятий практически любого сектора экономики: топливно-энергетического комплекса, металлургической промышленности, химической промышленности и др. [2–4].

Необходимо принять во внимание, что исторически при создании АСУ ТП использовались разработки, сделанные по индивидуальному заказу с применением специализированных протоколов и средств связи без каких-либо средств защиты информации. В то же время

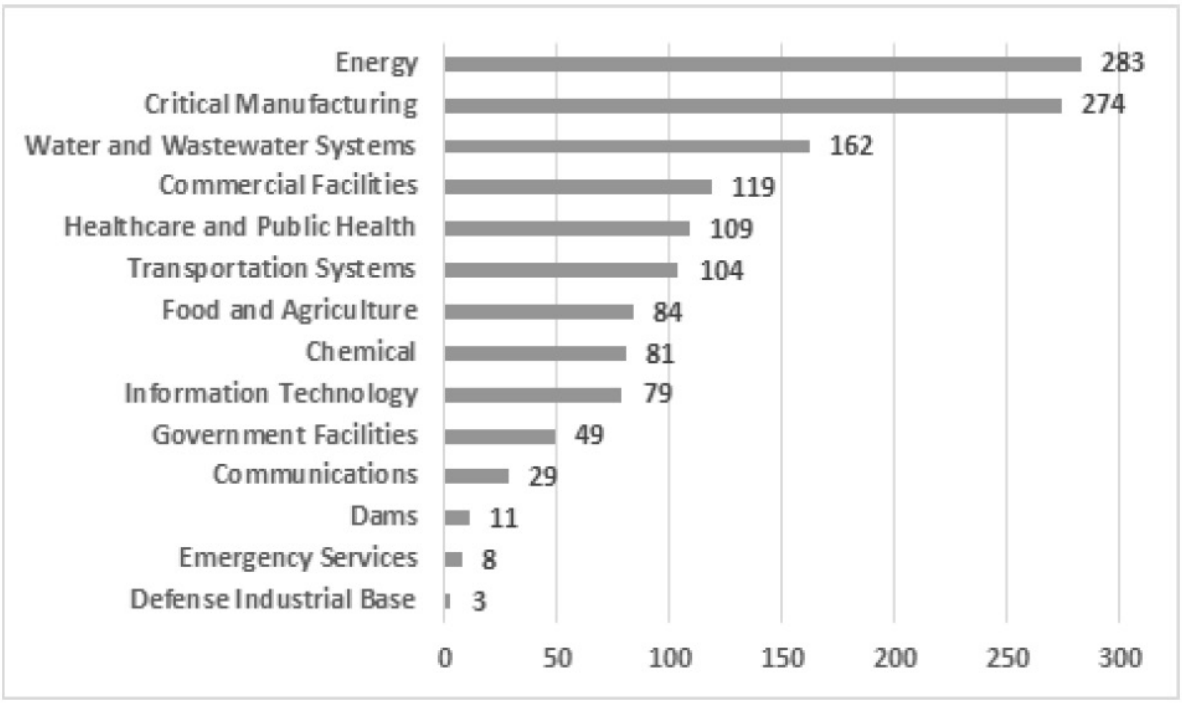

Рис. 1. Уязвимости, опубликованные за 2019 год [1]

тенденция цифровизации процессов в АСУ ТП приводит к расширению объема и разнообразия используемой в АСУ ТП информационной инфраструктуры, платформ, приложений и устройств. В АСУ ТП используется все больше современных технологий, таких как облачные технологии, интернет вещей (IoT), в том числе промышленный интернет вещей (IIoT) [5], искусственный интеллект (AI). Проблема заключается в том, что современный уровень развития информационных технологий и их проникновение в АСУ ТП несет не только новые возможности для автоматизации и управления технологическими процессами предприятия, но и новые угрозы и риски ИБ [6].

В последние годы множество стран разрабатывают технологии кибернетических атак, которые отличаются скрытностью и эффективностью, позволяя нарушать работу систем, автоматизирующих критически важные процессы — от АСУ ТП промышленных предприятий до систем жизнеобеспечения городов.

Целью данной работы является критический анализ программно-аппаратных комплексов обеспечения защиты критической информационной инфраструктуры и выработка предложений по их совершенствованию.

Проблематика

При обеспечении информационной безопасности АСУ ТП на первое место выходят свойства целостности и доступности информации. Искажение информации, поступающей с датчиков и устройств телеметрии, может привести к принятию неверного решения оператором или средством автоматизации, что существенно повышает вероятность реализации техногенных угроз различной степени тяжести. Также очевидным является требование по необходимости обеспечения высокого уровня доступности информации, циркулирующей в АСУ ТП, особенно в АСУ ТП с наличием обратной управляющей связи.

Усложнение применяемых информационных технологий и процессов функционирования АСУ ТП приводит к тому, что потенциальные нарушители получают значительно более широкий спектр возможностей по деструктивному воздействию на АСУ ТП путем использования ошибок и недекларированных возможностей аппаратно-программных средств, применяемых в составе АСУ ТП. Отсутствие четко выраженной экспликации стратегии защиты АСУ ТП приводит к снижению уровня доверия к средствам автоматизации и современным системам, используемым при управлении технологическими процессами, что в целом снижает эффективность работы и уровень безопасности предприятия.

Отчеты ведущих профильных исследовательских центров показывают, что в 2019 году было выявлено существенно количество инцидентов ИБ в сфере АСУ ТП, включая атаки с использованием кибероружия, направленные на конкретное оборудование промышленных

Таблица 1. Распределенные уязвимости по степени рисков

Оценка степени риска	9–10 (критическая)	7–8,9 (высокая)	4–6,9 (средняя)	0–3,9 (низкая)
Кол-во уязвимостей	97	249	143	18

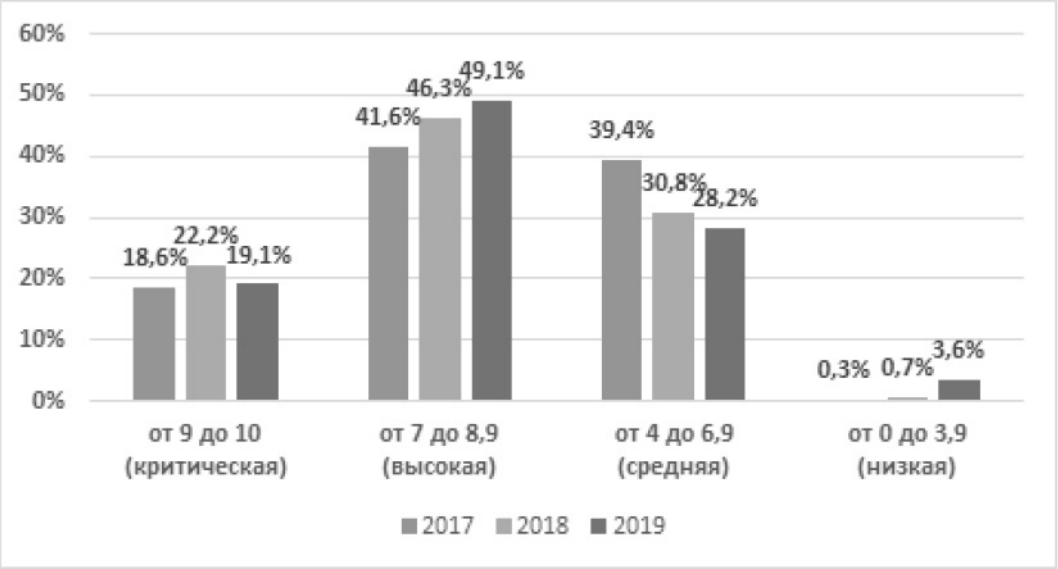

Рис. 2. Процент уязвимостей по степени риска, 2019 в сравнении с 2017 и 2018 годами

систем автоматизации. В частности, об этом свидетельствуют полугодовые отчеты Лаборатории Касперского [1], периодические отчеты ICS-CERT (Центра реагирования на инциденты информационной безопасности в АСУ ТП) [2] и ежегодный аналитический отчет от российской компании Positive Technologies [3]

На рис. 1 представлено количество уязвимых продуктов, используемых в различных отраслях (по классификации US ICS-CERT).

В 2019 году больше половины уязвимостей АСУ ТП получили свыше 7 баллов по CVSS версии 3.0, что соответствует высокому и критическому риску. В табл. 1 представлены опубликованные уязвимости по степени риска.

Если сравнивать с 2017 и 2018 годом, то доля уязвимостей, имеющих высокую и критическую оценку риска возросла (рис. 2).

Для повышения уровня обеспеченности стратегической безопасности объектов критической информационной инфраструктуры Российской Федерации требуется создание программно-аппаратных комплексов, направленных на предотвращение потенциальных киберугроз. При этом российские и зарубежные организации-производители средств защиты ведут постоянную работу по созданию решений для обеспечения ИБ промышленных систем автоматизации и управления (ПСАиУ), учитывающих специфику промышленных сетей и оборудования.

В данной статье рассмотрим лучшие программно-аппаратные решения для обеспечения ИБ ПСАиУ, проведем анализ их недостатков и сформируем предложения по их совершенствованию.

Предметное решение

Рассмотрим актуальные российские и зарубежные решения для обеспечения ИБ ПСАиУ и их состав:

- Indegy [4] — комплекс решений, объединяющих в себе группы безопасности и операции с полной видимостью, безопасностью и контролем активности и угроз промышленных систем управления, сочетающее гибридный мониторинг на основе политик безопасности и обнаружения аномалий сети с проверками целостности.

Таблица 2. Сравнение функциональных возможностей программно-аппаратных решений обеспечения ИБ ПСАиУ

Параметр сравнения	Зарубежные программные продукты					Отечественные программные продукты			
	Indegy	Industrial Defender ASM	CyberX	SCADA guardian	Dragos	ARMA	KICS	DATARK	ISIM
1	3	4	5	6	7	8	9	10	11
Возможное влияние на защищаемую систему									
Установка программной части на компоненты АСУ ТП	-	+	-	-	-	+	+	-	-
Требуется разрыв канала (сетевой, физический, канальный уровень)	-	-	-	-	-	+	-	-	-
Есть ли блокирующие функции влияющие на целостность АСУ ТП	-	-	+	+	-	+	+	-	-
Характеристика интерфейса управления									
Графический WEB-интерфейс управления	+	+	+	+	+	+	-	+	+
Интерфейс командной строки	-	-	-	-	-	-	-	-	-
Упрощенный интерфейс	-	-	-	-	-	-	-	-	-
Механизмы контроля целостности технологической сети									
Автоматическая идентификация узлов сети	+	-	+	+	+	-	-	+	+
Возможность дальнейшего мониторинга	-	-	+	+	+	-	-	+	+
Автоматическое формирования профиля сетевой активности АСУ ТП	-	-	+	+	+	+	-	-	-
Сбор и анализ событий ИБ									
Статические правила корреляции	+	+	+	-	+	-	+	+	+
Построение нормального профиля событий ИБ и анализ отклонений	-	-	-	-	-	-	-	-	-
Анализ защищенности									
Анализ уязвимостей по описаниям известных уязвимостей на стандартизированном языке OVAL	-	-	-	-	-	-	-	+	-
Контроль соответствия требованиям, описанным на стандартизированном языке OVAL	-	-	-	-	-	-	-	+	-
Управление инцидентами ИБ									
Система управления инцидентами ИБ	-	-	-	-	-	-	-	-	-
База знаний инцидентов ИБ в АСУ ТП	-	-	-	-	-	-	-	-	-
Поддержка принятия решений	-	-	+	+	-	-	-	-	-

- Industrial Defender ASM [5] — платформа управления, разработанная для удовлетворения перекрывающихся требований кибербезопасности, соответствующая требованиям и управления изменениями для промышленных систем управления.
- CyberX [6] — решение для автоматического обнаружения активов, выявления критических уязвимостей и векторов атак и постоянного мониторинга промышленных сетей кибербезопасности на наличие вредоносных программ и целевых атак.
- SCADA guardian [7] — комплексное решение по обнаружению кибератаки и аномалии процессов, предоставляя информацию, которая улучшает кибер-устойчивость, надежность и безопасность.
- Dragos [8] — комплексное решение для управления инцидентами и событиями безопасности, специально разработанное для промышленных сред, и может быть развернуто в модели центра операций безопасности.
- ARMA — программно-аппаратный комплекс с межсетевым экраном для выявления и блокировки кибератак на АСУ ТП.
- KICS — комплексное решение для делегирования аномальной активности в индустриальной сети, своевременного обнаружения и расследования инцидентов ИБ.
- DATAPK — комплекс DATAPK обеспечивает оперативный мониторинг и контроль состояния защищенности автоматизированных систем управления технологическими процессами (АСУ ТП).
- ISIM — система управления инцидентами кибербезопасности АСУ ТП, которая выявляет хакерские атаки и помогает в расследовании инцидентов на критически важных объектах.

Для проведения сравнительного анализа в качестве параметров определены характеристики, влияющие на возможные ограничения при использовании решений в рамках АСУ ТП, определяющие полноту собираемой с ПСАиУ информации и позволяющие оценить возможность реализации комплексного подхода по обеспечению ИБ ПСАиУ.

Параметры для сравнения сгруппированы в следующие блоки:

- Возможное влияние на защищаемую систему;
- Характеристика интерфейса управления;
- Механизмы контроля целостности технологической сети;
- Сбор и анализ событий ИБ;
- Анализ защищенности;
- Управление инцидентами ИБ.

В таблице 2 представлено сравнение функциональных возможностей программно-аппаратных решений обеспечения ИБ ПСАиУ.

Проведенный анализ позволяет сделать вывод о необходимости совершенствования средств защиты объектов критической информационной инфраструктуры, в частности были выявлены недостатки в существующих программно-аппаратных комплексах:

1. отсутствие упрощенного интерфейса, что требует специализированных знаний у работников;
2. отсутствие возможности анализа уязвимостей по описаниям известных уязвимостей на стандартизированном языке OVAL;
3. отсутствие возможности построения нормального профиля событий ИБ и анализ отклонений;
4. отсутствие возможности контроля соответствия требованиям, описанным на стандартизированном языке OVAL;
5. отсутствие встроенной системы управления инцидентами ИБ или возможности интеграции с внешней системой УИБ;
6. отсутствие базы знаний инцидентов ИБ в АСУ ТП;
7. отсутствие поддержки принятия решений.
8. отсутствие возможности вывода наглядной информации об уровне риска.

Каждый из рассмотренных программно-аппаратных комплексах обладает какими-либо из отмеченных недостатков. Данные недостатки могут критически сказаться на защищенности АСУ ТП. Например, для оценки уровня риска в простейшем случае производится оценка двух факторов [9]:

- вероятность происшествия;
- тяжесть возможных последствий.

Общий смысл оценки риска может быть выражен следующей формулой:

[уровень риска ИБ]=[вероятность происшествия]* [цена потери]

Обязательным критериями разработки программно-аппаратных комплексов должно быть соответствие российскому законодательству, в частности отсутствие недекларированных возможностей, наличие аттестатов соответствия и вхождение в реестр российского программного обеспечения. Лидерами российского рынка в области создания средств защиты информационной безопасности являются АО «Позитив Текнолоджиз», АО «Лаборатория Касперского», ЗАО «Инфовотч», ООО «УЦСБ», полноценно отвечающие заявленными требованиями к компаниям разработчикам. Модернизация средств защиты позволит повысить уровень стратегической безопасности объектов критической информаци-

онной инфраструктуры Российской Федерации, особенно в период цифровой трансформации экономики.

Заключение

Данная работа раскрывает проблему повышения уровня стратегической безопасности объектов критической информационной инфраструктуры. Важность указанной проблемы связана с происходящей в настоящее время цифровизацией экономики. Реализация киберугроз в отношении объектов критической информационной инфраструктуры способна как нанести существенный урон отдельных предприятиям, таки полностью парализовать жизнедеятельность целых городов. В работе проведен сравнительный анализ программно-аппаратных комплексов обеспечения защиты критической информационной инфраструктуры. Выявлен перечень недостатков в существующих программно-аппаратных комплексах, исходя из специфики требований обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации.

ЛИТЕРАТУРА

1. Юршев А.Ю., Смирнов М. Б. Вопросы выбора средств защиты для АСУ ТП и значимых объектов КИИ. Защита информации. Инсайд. 2019; 1(85): 4–7.
2. Ильченко Л.М., Галлямова М. Р., Юрин И. В., Зайцев С. И. Определение значимых процессов критического объекта информационной инфраструктуры российской федерации на примере телекоммуникационного предприятия. Проблемы информационной безопасности. Компьютерные системы. 2019; 2: 107–116.
3. Гулиев И.А., Рузакова В. И. Защита целостности критической инфраструктуры компаний ТЭК как вызов цифровой экономики. Экологический вестник России. 2019; 12: 26–29.
4. Глухов А.П., Василенко В. В., Сидак А. А., Ададуров С. Е., Белова Е. И. Определение уровня безопасности значимых объектов критической информационной инфраструктуры железнодорожного транспорта. Двойные технологии. 2020; 1(90): 84–88.
5. Дахнович А.Д., Москвин Д. А. Метод безопасной трансформации инфраструктуры АСУ ТП в промышленный интернет вещей. Проблемы информационной безопасности. Компьютерные системы. 2019; 4: 92–100.
6. Калашников А.О., Аникина Е. В., Остапенко Г. А., Борисов В. И. Влияние новых технологий на информационную безопасность критической информационной инфраструктуры. Информация и безопасность. 2019; 22(2): 156–169.
7. Iskhakov A. Yu., Iskhakova A. O., Meshcheryakov R. V., Bendraou R., Melekhova O. Application of user behavior thermal maps for identification of information security incident // Труды СПИИРАН. 2018. № 6 (61). С. 141–171.
8. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2019. Version 1.0 — исследовательский центр Kaspersky lab ICS CERT [Электронный ресурс] //URL: https://ics-cert.kaspersky.ru/media/KASPERSKY_H22019_ICS_REPORT_FINAL_RU.pdf
9. Security Bulletins. [Электронный ресурс] // URL: https://www.us-cert.gov/ncas/bulletins.
10. Уязвимости в АСУ ТП: итоги 2018 года, подготовлен 11.04.2019 — исследовательский центр Positive Research (securitylab.ru/lab). [Электронный ресурс] // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-vulnerabilities-2019-rus.pdf.
11. Официальный сайт Indegy. [Электронный ресурс] // URL: https://www.tenable.com/
12. Официальный сайт Industrial Defender ASM. [Электронный ресурс] // URL: https://www.industrialdefender.com/industrial-defender-asm/.
13. Официальный сайт CyberX. [Электронный ресурс] // URL: https://cyberx-labs.com/.
14. Официальный сайт SCADA guardian. [Электронный ресурс] // URL: https://cyberx-labs.com/.
15. Официальный сайт Dragos. [Электронный ресурс] // URL: http://www.nozominetworks.com/.
16. Милославская Н.Г., Сенаторов М. Ю., Толстой А. И. Управление рисками информационной безопасности. //М: Научная библиотека ПНИПУ, 2014.

© Фомин Николай Александрович (science-fomin@yandex.ru),
Самошина Анна Ивановна (ania.cat03@gmail.com), Евсютин Олег Олегович (evsutin.oo@gmail.com),
Домуховский Николай Анатольевич (ndomukhovsky@ussc.ru), Комаров Денис Евгеньевич (dkomarov@ussc.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»