



Аналитический отчет

**Тенденции развития
киберинцидентов
АСУ ТП
за 2023 год**



Оглавление

Сокращения	3
Аннотация	4
Объекты атак.....	5
Методы атак.....	6
ВПО, применяемое для атак на АСУ ТП.....	8
Основные группировки, атакующие АСУ ТП.....	9
Приоритеты в кибербезопасности АСУ ТП	14
Отраслевые тенденции.....	15
Выводы.....	19



Сокращения

AiTM	Adversary-in-the-middle "Противник посередине" – техника атак
C2	command and control – техника атак
CVE	Список уязвимостей информационной безопасности
CWE	Система классификации недостатков информационной безопасности
DDoS	Распределенный отказ в обслуживании — хакерская атака на вычислительную систему с целью довести её до отказа с помощью распределенной сети множества устройств, посылающих запросы
LotL	living off the land – техника атак
RaaS	Программа-вымогатель как услуга
RDP	Протокол удаленного рабочего стол
VPN	Виртуальные частные сети
АСУ ТП	Автоматизированная система управления технологическими процессами
ИБ	Информационная безопасность
ВПО	Вредоносное программное обеспечение
ПЛК	Программируемый логический контроллер
ПО	Программное обеспечение



Аннотация

Экспертно-аналитический центр ГК InfoWatch представляет отчёт по результатам исследования тенденций развития киберинцидентов систем управления технологическими процессами в мире.

В последние годы наблюдается рост атак на АСУ ТП не только со стороны вымогателей, но также со стороны группировок, нацеленных на причинение промышленному предприятию или энергетической компании максимального ущерба. Также растет количество случаев кибершпионажа.

Различные отчеты и обзоры по тематике информационной безопасности АСУ ТП носят достаточно фрагментарный характер.

Целью данного исследования являлось намерение консолидировать и систематизировать большую часть доступной информации для выявления ключевых тенденций и изменений.

В рамках данного исследования использовались в значительной мере собственные данные ГК InfoWatch, включая базу инцидентов в промышленности и энергетике, а также находящаяся в открытом доступе информация более чем от:

- 150 вендоров ИБ АСУ ТП,
- 30 аналитических и консалтинговых компаний,
- 40 промышленных ассоциаций,
- 50 информационных агентств в сфере информационных и операционных технологий,
- 30 крупнейших сервис-провайдеров.

В исследовании приведены обобщенные данные по итогам анализа собранной информации, проведены анализ распределения атак на АСУ ТП по источникам и методам атак, анализ наиболее атакуемых устройств АСУ ТП, типов применяемого вредоносного программного обеспечения. Приведены тактики основных группировок, атакующих АСУ ТП. Рассмотрены тенденции технологических приоритетов развития ИБ АСУ ТП у предприятий, а также отраслевые тенденции.

Отчет будет полезен специалистам по информационной безопасности, в том числе по информационной безопасности АСУ ТП, а также специалистам в области АСУ ТП и промышленного интернета вещей.



Объекты атак

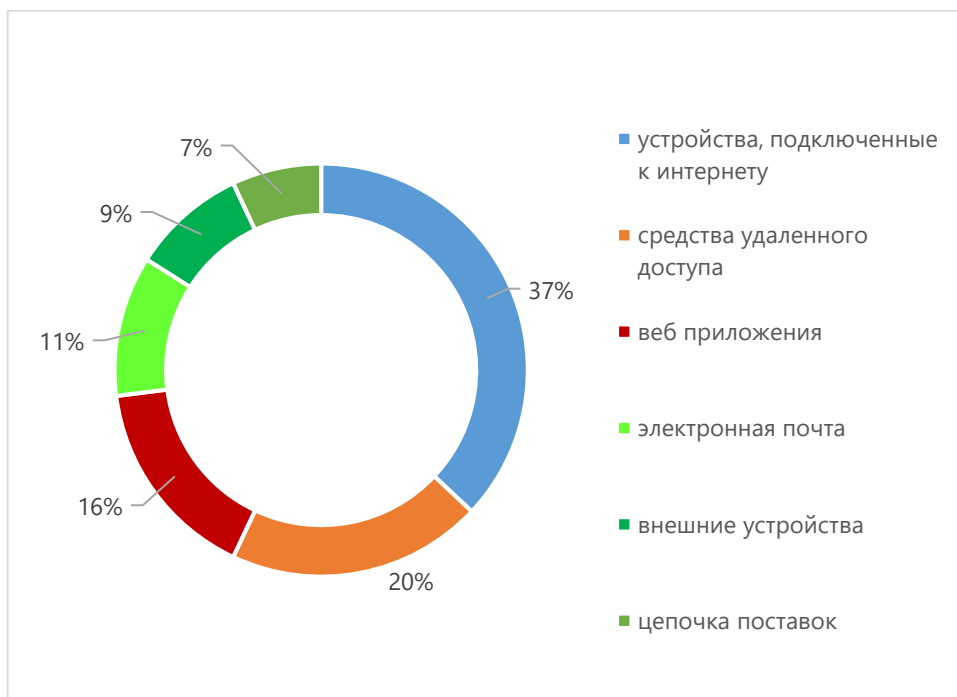


Рис 1. Распределение атак по источникам в 2023 г.

Основная доля атак на АСУ ТП направлялась из интернета. В 2023 г. в качестве меры обеспечения кибербезопасности отмечен рост изоляции устройств АСУ ТП от внешних подключений. Если в 2021 г. более 70% устройств АСУ ТП имело подключения к сети Интернет, то в 2023 г. меньше половины.

В 2023 г. отмечен рост использования атакующими протокола удаленного рабочего стола (RDP) и виртуальных частных сетей (VPN), рост использования атакующими ПО удаленного мониторинга и управления (RMM). Ожидается, что ввиду распространения этого ПО у многочисленных сервис-провайдеров, эта тактика будет развиваться.

Отмечается рост атак на АСУ ТП с использованием «старых» методов - living off the land (LOTL), Golden SAML, command and control (C2).

Рост атак через **удаленное подключение** связан с тем, что компании часто размещают модемы сотовой связи в удаленных местах, где проводное подключение непрактично или неэкономично. Устройства, к которым подключают модемы, используются коммунальными службами для размещения на насосных станциях, резервуарах для хранения и подъемных станциях, небольших гидроэлектростанциях, распределенных солнечных установках и хранилищах в системах генерации электроэнергии. Важно, что модемы обычно подключаются напрямую к устройствам АСУ ТП, подвергая их угрозам.

Программируемый встроенный веб-сервер, где пользовательский клиентский JavaScript-код использует все более мощные интерфейсы **веб-приложений** для



мониторинга и управления физическими процессами, создает идеальную платформу для запуска ВПО для ПЛК, что представляет растущую угрозу АСУ ТП. Дополнительным преимуществом подобного применения ВПО является то, что, несмотря на то, что оно разворачивается на ПЛК, запускается ВПО только в веб-браузерах, используемых для управления функциями ПЛК. Тогда как типичные подходы борьбы с ВПО основаны на изучении самих ПЛК на предмет обнаружения аномалий, а не веб-браузеров.

В 2023 г. отмечен рост **фишинга как услуги** (phishing-as-a-service, PhaaS) с использованием метода Adversary-in-the-middle "Противник посередине" (AiTM). Растет размещение фишинговых URL-адресов у поставщиков облачных услуг, таких как Adobe, Dropbox, Google и Microsoft. После многократных перенаправлений жертвы попадают на конечную целевую страницу, которая крадет учетные данные или загружает ВПО на их компьютер.

Эксперты сообщают о ВПО - платформе **Incontroller framework**, модульном наборе инструментов, позволяющим выдавать команды для изменения конфигураций ПЛК, манипулирования выходными данными, внедрения бэкдоров, инициирования DoS-атак.

Методы атак



Рис 2. Наиболее распространенные методы атак на АСУ ТП в 2023 г.

Уязвимость устройств АСУ ТП для атак обусловлена их специфичностью, отсутствием обновлений (чаще – отсутствием установки появляющихся обновлений в связи с опасениями, что они могут нарушить работоспособность установки, а стенды для проверки обычно отсутствуют), проблемами конвергенции с ИТ инфраструктурой.



75-80% устройств АСУ ТП имеют известные уязвимости. 45-50% уязвимостей не поддаются исправлению ввиду использования на предприятиях неподдерживаемых систем. Вследствие чего хакеры часто эксплуатируют уязвимые устройства АСУ ТП при помощи инструментов поиска в Интернете, чтобы найти порты для удаленного управления и получить несанкционированный доступ, часто применяя учетные данные по умолчанию.

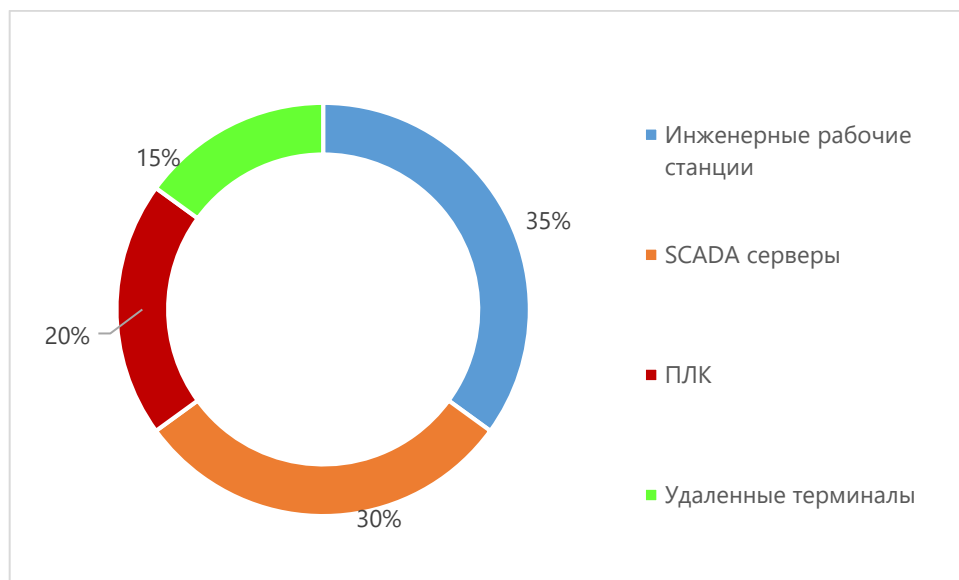


Рис 3. Наиболее атакуемые устройства АСУ ТП

Аналитики прогнозируют, что количество предупреждений об уязвимостях, относящихся к промышленным операциям, удвоится в ближайшие пять лет. Такой быстрый рост числа уязвимостей объясняется тем, что поставщики и исследователи уделяют больше внимания безопасности АСУ ТП, чем раньше.

Ожидается, что тенденция будет усиливаться с акцентом на использование конфигураций облачной инфраструктуры.

Наблюдается постоянный рост использования уязвимостей нулевого дня и 2023 год близок к тому, чтобы побить предыдущий рекорд, установленный в 2021 году. Ожидается, что в 2024 году будет больше случаев использования "нулевого дня" различными группировками.

Уязвимости, связанные с несанкционированным чтением и записью, являются наиболее эксплуатируемыми в атаках на АСУ ТП. Только в 2023 году сообщалось о двенадцати уязвимостях (CVE), связанных с CWE-787, которые могут использоваться при атаках.

Внедрение команд операционной системы стало в 2023 г. второй наиболее активно эксплуатируемой уязвимостью CWE. Уязвимость позволяет злоумышленнику манипулировать вводимыми данными таким образом, что приложение совершает неверные команды в системе.



Компания Palo Alto Networks, один из мировых лидеров в разработке межсетевых экранов и облачных решений по кибербезопасности, сообщила, что CVE-2022-29303 использовался для распространения различных видов ботнета Mirai. CVE-2022-29303 повлиял на CONTEC SolarView, систему мониторинга энергопотребления, которая через веб-сервер, загрузила Mirai 5.

Уязвимости обхода пути CWE-22 были одними из наиболее распространенных типов уязвимостей в 2023 году. Как правило, эти уязвимости затрагивают веб-серверы и другие приложения, которые взаимодействуют с локальной файловой системой устройства, хоста или сервера. Они также часто влияют на инженерное программное обеспечение, где файлы проекта содержат пути к файлам как часть архива.

Широкое использование CODESYS - инструментального ПО промышленной автоматизации, который производится и распространяется компанией 3S-Smart Software Solutions GmbH обуславливает появление рисков, связанных с уязвимостями цепочки поставок для АСУ ТП. Уязвимости CODESYS позволяют проводить DDoS атаки, создавать бэкдор для ПЛК, для изменения работы ПЛК и шпионажа.

ВПО, применяемое для атак на АСУ ТП

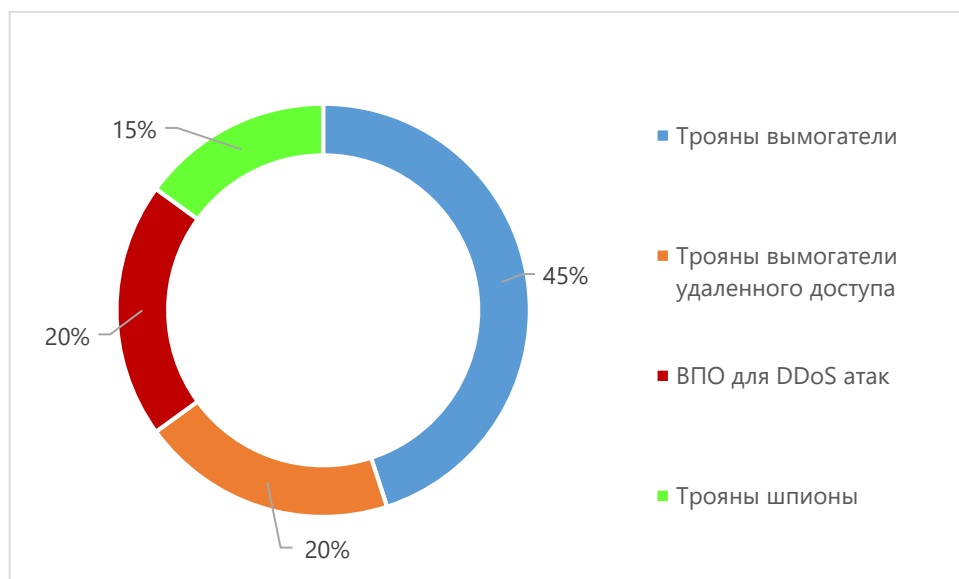


Рис 4. ВПО, атакующее АСУ ТП, 2023 г.

Вирусы вымогатели

Количество атак программ-вымогателей на АСУ ТП выросло, по разным оценкам, на 50%- 70% в 2023 году. Ожидается, что рост продолжится в 2024 году.

Ключевые тенденции 2023:

- Нацеливание на критически важную инфраструктуру.



- Рост использования программ-вымогателей как услуги (RaaS).
- Рост использования тактики двойного вымогательства, когда злоумышленники шифруют и крадут данные жертв, требуя денег как за дешифровку, так и за то, что данные не будут опубликованы.
- Рост количества атак программ-вымогателей, управляемых человеком, более чем в три раза.
- Резкий рост использования систем удаленного шифрования. В 2023 году около половины вирусов-вымогателей, управляемых человеком, использовали удаленное шифрование.
- В атаках на АСУ ТП лидирует LockBit, вымогатель, управляемый человеком, на него приходится более четверти атак в 2023 г.

DDoS атаки

Ключевые тенденции 2023 г.:

- Рост DDoS-атак по найму. Разработчики предоставляют подписки на booter'ы и стрессеры, с помощью которых можно вывести из строя веб-сайты и сети.
- Рост использования ресурсов облачных вычислений, таких как виртуальные машины, для запуска DDoS-атак. Так, в 2023 году хакеры ориентировались на льготные подписки Azure в различных регионах, создав множество учетных записей в 40 из 59 региональных покрытий Azure.
- Рост многовекторных атак, мощности и продолжительности атак.

Основные группировки, атакующие АСУ ТП

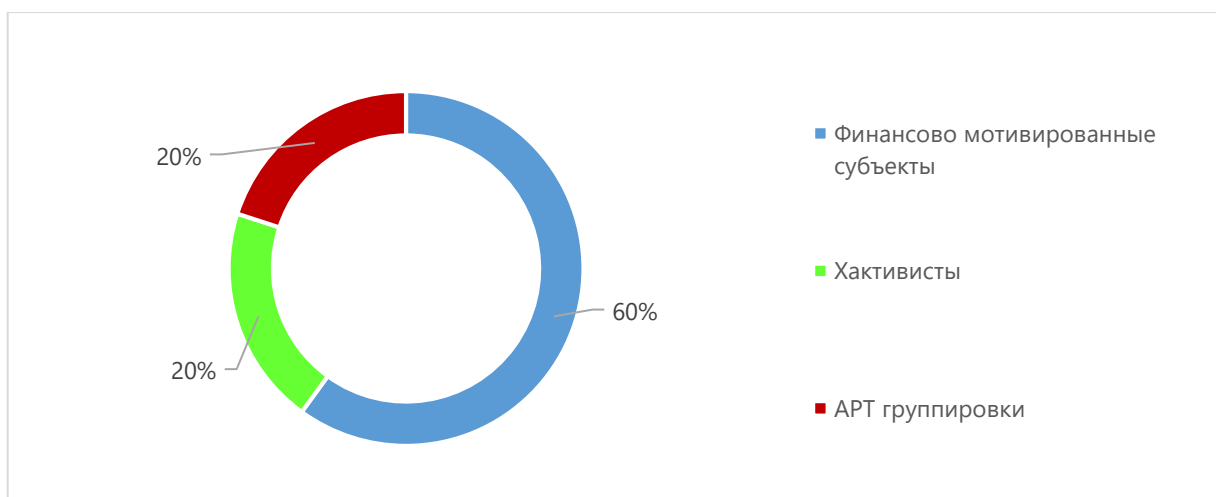


Рис 5. Атаки по типам группировок на АСУ ТП, 2023 г.



- **Финансово мотивированные субъекты** - группы, руководимые преступной организацией/лицом с мотивацией получения финансовой выгоды, которые не связаны с государством или коммерческой организации. в основном фокусируются на вымогательстве, выполнении заданий по борьбе с конкурентами, промышленном шпионаже.
- **APT (Постоянная серьезная угроза англ. advanced persistent threat) – группировки.** После громких кибератак 2022 года хакеры снизили количество масштабных разрушительных атак и вместо этого направили основную часть своей деятельности на кибершпионаж. В то же время, по мере развития ландшафта угроз, наблюдается стирание границ между кибероперациями, шпионажем, кампаниями влияния и деструктивными атаками
- **Хактивисты.** Группировки преследуют различные политические, экологические, идеологические цели, могут заниматься, как диверсионной деятельностью, так и вымогательством.

Основные группировки, атакующие АСУ ТП

Группа	Цели	Методы
LockBit	вымогательство как услуга	Поставщик StealBit, инструмента для кражи информации, программы-вымогателя как услуги (RaaS).
ALPHV	вымогательство как услуга	ALPHV (BlackCat) считается преемником операторов ransomware REvil, DarkSide и BlackMatter. Поставщик программы-вымогателя как услуги (RaaS).
BlackBasta	вымогательство	Используют практику двойного вымогательства – шифрование с требованием выкупа, похищение данных с угрозой опубликования.
VOLTZITE	кража учетных данных, долгосрочный шпионаж, деструктивное воздействие	Активно использует методы living off the land (LOTL) и, в некоторых случаях, было замечено, что он выполняет действия по компрометации сообщений “с клавиатуры” в сетях жертвы. делает попытки закрепиться на сетевом периметре цели, чтобы затем получить возможность



		дальнейшего проникновения в сеть информационных технологий жертвы, а затем переместиться в сеть АСУ ТП. Использует протокол удаленного рабочего стола (RDP) и атаки с обходом каталога. Также VOLTZITE пересекается с инфраструктурой, связанной с ботнетом Mirai.
Peach Sandstorm	шпионаж	Тактика распыления паролей и индивидуальные инструменты для эксфильтрации данных, использует AnyDesk (RMM), проводит атаки Golden SAML, использует EagleRelay для туннелирования трафика обратно в свою инфраструктуру, используют действия по удалению паролей, внутреннюю разведку с помощью AzureHound или Roadtools, множественные механизмы сохранения и удаленную эксплуатацию уязвимых интернет-приложений.
CyberAv3ngers	деструктивное воздействие	Сканирование открытого Интернета, чтобы идентифицировать общедоступные устройства Unitronics, а затем попытки входа, используя пароль Unitronics по умолчанию.
Gananite	шпионаж, кража данных	Использование StinkRAT и общедоступных proof of concept эксплойтах для конечных точек, также демонстрирует использование таких инструментов, как TELEMIRIS и JLORAT, использует поисковые системы Shodan и FOFA, которые содержат данные об активах, подключенных к Интернету, для создания профиля своей цели.



Chernovite	деструктивное воздействие	Является разработчиком PIPE DREAM, ПО фокусируется на нарушении работы АСУ ТП, использует протоколы, специфичные для АСУ ТП, для разведки, манипулирования и отключения ПЛК, захвата учетных данных ПЛК.
Sandworm	шпионаж, деструктивное воздействие	Использование living off the land (LotL) АСУ ТП уровня для разрушения среды ОТ, использование CADDYWIPER с помощью двух GPO с контроллера домена с использованием TANKTRAP - утилиты, написанной на PowerShell, которая использует групповую политику Windows для распространения и запуска wiper/вайпера (ВПО, стирающего данные, без возможности восстановления). Эксперты наблюдали, как TANKTRAP использовался с другими инструментами, включая NEARMISS, SDELETE, PARTYTICKET и CADDYWIPER.
Bentonite	деструктивное воздействие	Использует уязвимости в ресурсах, подключенных к Интернету, фокусируясь на уязвимостях Log4j и VMware Horizons. Интенсивное использование Powershell для облегчения компрометации. Отдельные домены для фишинга и C2. Использует Github для доставки, SSH и HTTP для C2.
Kostovite	шпионаж, деструктивное воздействие	Использование уязвимости нулевого дня в Citrix.
Kamacite	деструктивное воздействие, помощь другим группировкам	ВПО CYCLOPS BLINK, направлено на маршрутизаторы малого офиса/домашнего офиса (SOHO) и сетевые хранилища данных.



Xenotime	деструктивное воздействие, помощь другим группировкам	Компрометация и нарушение работы систем промышленной безопасности (SIS).
Electrum	деструктивное воздействие	Внедрение INDUSTROYER2, ВПО, специфичного для АСУ ТП.
Wassonite	деструктивное воздействие	ВПО написано на языке Hangul для создания многокомпонентного бэкдора, который может делать скриншоты, регистрировать нажатия клавиш и собирать информацию о съемных носителях и файлах конкретных жертв. Он также может загружать, выгружать и выполнять последующие команды с сервера команд и контроля (C2).
Hellhounds	шпионаж	Троян удаленного доступа.
Laurionite	шпионаж, деструктивное воздействие	Нацелен на веб-сервисы и активы Oracle E-Business Suite iSupplier.
Respite & Magnalium	деструктивное воздействие	Сканирование уязвимых устройств малого и среднего бизнеса и использование методов распыления паролей. После первоначального доступа и разведки, группа развертывала wiper/вайпер.



Приоритеты в кибербезопасности АСУ ТП

Расходы на обеспечение информационной безопасности (кибербезопасности) АСУ ТП в мире в 2023 году составили 9 миллиарда долларов. При совокупном среднегодовом росте в 18% объем рынка утроится к 2030 году, достигнув 27 миллиардов долларов. Ожидается, что рынок может достигнуть величины в 150-225 миллиардов долларов. Количество новых патентов по ИБ АСУ ТП и Промышленного Интернета вещей растет с совокупным среднегодовым темпом роста в 25-30%.



Рис 6. Приоритеты в кибербезопасности АСУ ТП у конечных пользователей в 2023 г.

Актуализация активов

Обеспечение доступности активов (устройств АСУ ТП) путём их мониторинга остается ключевой целью для предприятий и отправной точкой для программ обеспечения безопасности. Около 75-80% промышленных компаний имеют ограниченный мониторинг активов АСУ ТП в корпоративной системе ИБ, или он отсутствует. Инновации включают интеграцию с CMDB-базой данных управления конфигурациями, содержащую информацию об активах, использование машинного обучения для автоматической классификации активов, обнаружения изменений конфигурации или отклонений от базовой линии. Инновации машинного обучения также включают количественную оценку рисков и определение приоритетов действий.

Анализ угроз

В анализе угроз растет потребность в решениях, включающих в себя: возможность предоставлять необработанную телеметрию для глубокой аналитики, карты



моделирования атак, получение машиночитаемых данных анализа угроз в формате STIX/TAXII, мониторинг USB-портов.

Управление уязвимостями

В управлении уязвимостями передовые решения оценивают все активы, подключенные к сети, определяют приоритеты рисков и воздействия и предлагают стратегии исправления/смягчения последствий посредством настройки, обновления встроенного ПО и управления исправлениями. Поставщики отслеживают уязвимости через централизованные хранилища, такие как CVEs, NVD и NIST.

Сегментация сети

В сегментации сети будут востребованы решения, которые могут сравнивать ожидаемые и фактические конфигурации межсетевых экранов, согласовывать зоны и каналы с IEC-62443, рекомендовать конкретные политики, основанные на эксплуатации или отраслевом контексте.

Отраслевые тенденции

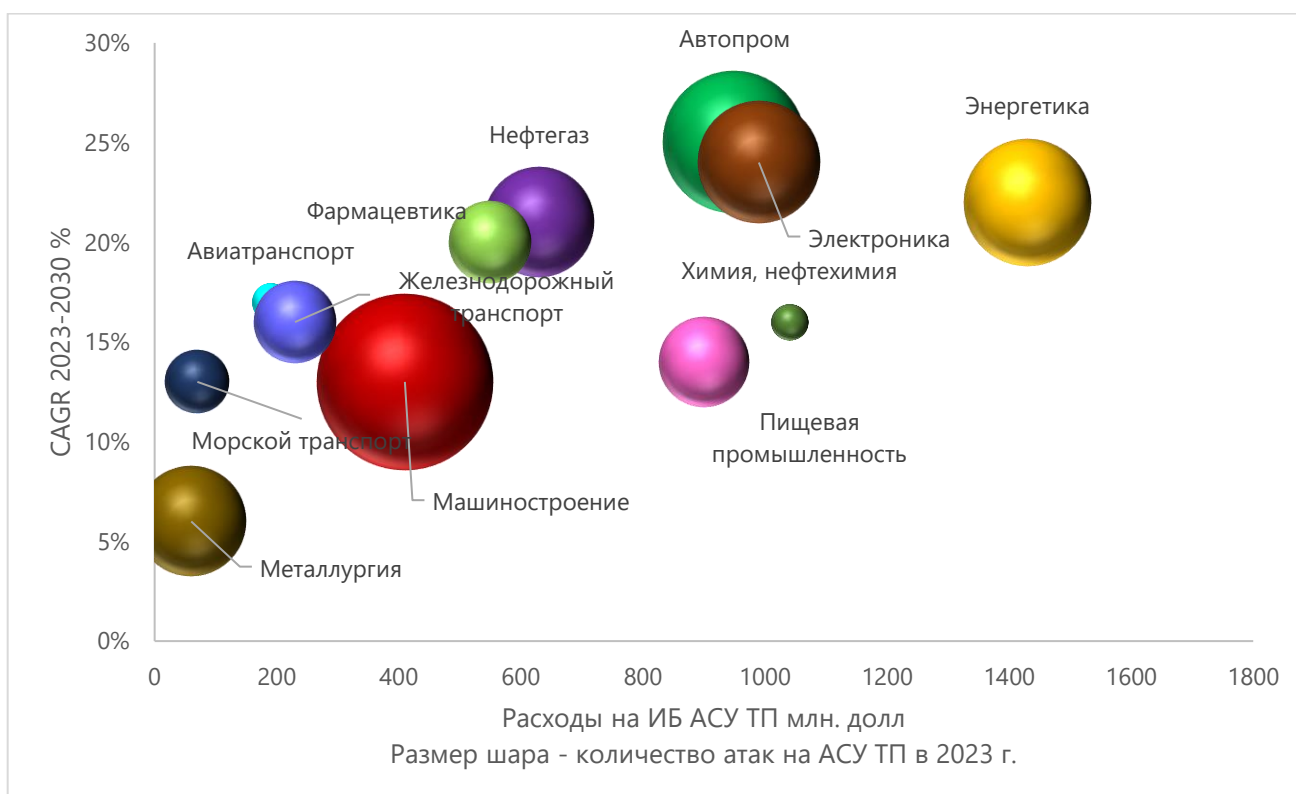


Рис 7. Рост затрат на ИБ АСУ ТП по отраслям 2023-2030 гг.

Инвестиции в кибербезопасность АСУ ТП ожидаются во всех секторах промышленности, причем все сегменты будут расти более чем на 5% в год к 2030 году.



Инвестиции стимулируются главным образом регулированием и цифровизацией промышленных операций. Энергетика (производство электроэнергии, передача и распределение) в последние годы находится под сильным влиянием регулирования практически во всех развитых государствах, поскольку является критически важной инфраструктурой, соответственно, государства требуют от энергетических компаний инвестировать в кибербезопасность. В отраслях производства с высокой добавленной стоимостью (автомобилестроение, фармацевтика, производство электроники) опережающими темпами развивается автоматизация и цифровизация. Инфраструктура информационных и операционных технологий увеличивается в разы, растет количество устройств, подключенных к интернету, значительно возрастают риски кибербезопасности. Компании опасаются не только атак вымогателей и деструктивного воздействия, но и кибершпионажа. Наибольшие инвестиции в кибербезопасность АСУ ТП приходятся на отрасли со сложными процессами и автоматизированные производственные процессы с высокой добавленной стоимостью.

Ключевые факторы, привлекающие хакеров

- Возможность хорошо заработать на вымогательстве, краже ноу-хау - автопром, фармацевтика, пищепром, химия/нефтехимия, нефтегаз, электроника.
- Возможность нарушить функционирование критически важной инфраструктуры или шантажировать этим, вымогая деньги или получая их от заказчиков (конкурентов, ОПГ, других государств), возможно, и в политических или общественных целях (хактивисты) - энергетика, водоснабжение, критически важное машиностроение
- Наличие значительной доли устройств с удаленным подключением на предприятиях с распределенной инфраструктурой АСУ ТП. Ограниченность мониторинга и преодоление, как правило, одного уровня защиты при взломе модема и подключенного к нему устройства, привлекают хакеров - нефтегаз, коммунальные службы, сельскохозяйственные предприятия, транспорт, уголь, лес.
- Расширенная цепочка поставок - сохраняется значительная разница между крупнейшими производителями, имеющими новые заводы, и большим количеством малых и средних предприятий, поставщиков компонентов, состоящих из небольших и специализированных производителей, уровень информационной безопасности которых значительно отстает от уровня обеспечения ИБ у производителей конечной продукции. То же относится и к дилерам предприятий. Взаимосвязанная информационная инфраструктура несет значительные риски информационной безопасности для головных предприятий - автопром, машиностроение в целом, электрика и электроника
- Низкий уровень инвестиций в информационную безопасность делает предприятие привлекательным для атаки, а также для атаки через него на другие компании, например, через производителей сельхозпродукции на предприятия



пищевой промышленности - сельскохозяйственные предприятия, поставщики компонентов, дилерские организации

- Разнообразие систем управления - морской транспорт. Атака может быть нацелена не на одного конкретного владельца или оператора, а на множество транспортных средств определенного типа, одинаковых или сходных с точки зрения внутренних систем управления. Фактором, упрощающим атаку, является оснащение судов кастомизированными системами сбора телеметрии с возможностями удалённого управления.

Перспективные угрозы

Использование хакерами изысканий исследователей

В то время как злоумышленники внедряют новые методы, чтобы избежать обнаружения, ожидается, что некоторые участники возрождают старые методы, которые широко не освещались. Например, в 2013 году исследователь написал сообщение в блоге об использовании недокументированных системных функций, вместо криптографических функций в документированном Windows API. Этот метод не был популярным до 4 квартала 2022 года, когда несколько исследователей безопасности начали обсуждать его и публиковать фрагменты кода в своих блогах и на GitHub. После этого образцы вредоносных программ, реализующие этот метод, начали появляться на VirusTotal. Также замечено использование в 2023 г. метода защиты от виртуальных машин (anti-VM), подробно описанного в книге по анализу вредоносных программ за 2012 год. Вероятно, таким же образом хакеры получают доступ и к новейшим разработкам исследователей, изначально направленных на создание перспективных средств защиты АСУ ТП и ИТ инфраструктуры.

Продолжающаяся миграция ВПО на современные языки программирования

Продолжающаяся миграция ВПО на современные языки программирования.

Авторы вредоносных программ продолжают разрабатывать больше программного обеспечения на таких языках программирования как Go, Rust и Swift. Это связано с тем, что языки обеспечивают отличный опыт разработки, большую стандартную библиотеку и легкую интеграцию со сторонними пакетами. Эти языки и экосистемы обеспечивают быструю разработку сложного ВПО, удешевляя его написание.

Более качественная подготовка к атакам

При атаке на АСУ ТП хакеры уделяют значительное внимание уклонению от обнаружения и сложным методам обеспечения оперативной безопасности, проводят длительную разведку цели, уделяя особое внимание краже учетных данных, боковому перемещению, эксплуатируют устаревшие маршрутизаторы SOHO, используя их в качестве промежуточных звеньев для атаки на АСУ ТП.



Спящие ботнеты

Хакерские группы создают “спящие ботнеты” из уязвимых устройств Интернета вещей и устаревшего активного сетевого оборудования, используя смесь старых и новых эксплойтов. Эти “спящие ботнеты” будут использоваться по мере необходимости и уничтожаться после обнаружения или когда они перестанут быть полезными, что усложнит усилия по борьбе с ними. В начале этого года ботнеты атаковали водоснабжение малых городов США.

Нацеливание на космическую инфраструктуру

В 2024 году эксперты ожидают увидеть использование ВПО для компрометации космической и связанной с ней наземной инфраструктуры поддержки и каналов связи с целью перехвата данных, нарушения связи.

Атаки на 5G

Активное внедрение в промышленности частных сетей 5G несет в себе определенные риски.

Децентрализация безопасности. До появления 5G в сетях было меньше физических связующих звеньев, поэтому было проще обеспечивать их безопасность и поддерживать работоспособность. Для динамических программно-реализованных систем 5G нужно больше точек маршрутизации. И для обеспечения безопасности каждую из них нужно постоянно проверять, даже одно незащищенное звено может подорвать безопасность остальных компонентов сети.

Продолжение проблем в цепочке поставок

К 2030 году мы увидим все большую интеграцию компонентов и сервисов, объединенных в новые продукты. Поскольку рынок требует ускорения циклов выпуска продукта, компонентно-ориентированное программирование значительно увеличится, что приведет к повторному использованию кода и использованию библиотек с открытым исходным кодом. Хотя некоторые из этих компонентов будут регулярно проверяться на наличие уязвимостей, сочетание программного обеспечения, аппаратного обеспечения и кода на основе компонентов приведет к неконтролируемым взаимодействиям и к появлению новых и непредвиденных уязвимостей, создавая больше возможностей для злоумышленников скомпрометировать цепочку поставок со стороны поставщика и заказчика.

Интеллектуальные атаки с использованием генерирующих состязательных сетей (GAN)

Одним из примеров использования GAN может быть нацеливание на серверы, распространяющие исправления, с целью срыва запланированных обновлений. Из-за критичности устройств это может создать системный риск, приводящий к перебоям в работе, повреждениям, а также перехвату данных между устройствами партнеров.



Фокус атак будет все больше смещаться на ИТ-провайдеров

В ближайшие 10 лет технологическая взаимосвязанность будет усилена. Граница между физическим и киберпространством будет еще более размыта, поскольку такие инфраструктурные секторы, как транспорт, здравоохранение, электросети и промышленность все больше зависят от поставщиков ИКТ-услуг для подключения к Интернету и управления всеми коммуникациями между устройствами. Несмотря на то, что сейчас их ответственность за поддержание ИТ-инфраструктуры значительна, в ближайшие годы их значение возрастет еще больше.

Умные города являются примером того, какими еще более важными будут ИТ сети через 10 лет. Поэтому ИТ-провайдеры станут мишенями для киберпреступных группировок, для получения доступа к их сетям, конечным точкам, центрам обработки данных, или другим компонентам инфраструктуры ИКТ, что может нанести ущерб городам и целым регионам.

Выводы

Рост геополитической напряженности в мире в 2023 году привел к росту атак на различные организации, в особенности, с критически важной инфраструктурой и, в первую очередь, на промышленные предприятия и энергетические компании.

Одновременно с этим росли возможности группировок, нацеленных на вымогательство. Количество атак программ-вымогателей на АСУ ТП выросло, по разным оценкам, на 50%- 70% в 2023 году. Значительно выросло вымогательство с помощью троянов удаленного доступа. Ожидается, что рост продолжится в 2024 году.

В 2023 г. выросли предложения вымогательства как услуги, фишинга как услуги, DDoS-атак по найму.

Основная доля атак на АСУ ТП велась хакерами через сеть «Интернет».

Наиболее атакуемыми отраслями были машиностроение, автопром, производство электроники и полупроводников, металлургия, энергетика. Тогда как автопром, производство электроники и полупроводников и энергетика являются лидерами по расходам на ИБ АСУ ТП и темпам роста расходов, затраты в машиностроении и металлургии явно недостаточны на фоне растущего количества атак.

Основными приоритетами в кибербезопасности АСУ ТП у конечных пользователей в 2023 году были:

- актуализация активов/видимость (около 70-80% устройств АСУ ТП не визуализируются),
- оценка рисков и управление уязвимостями,
- обнаружение и предотвращение угроз.

В 2024 г. мы будем наблюдать рост атак вымогателей на промышленные предприятия, будет расти кибершпионаж, а также деструктивные действия с целью остановки



деятельности предприятий, распространения негативного воздействия на целые отрасли.

Атаки возможны на новые сегменты, наиболее уязвимые для вторжений, такие как морской транспорт, сельскохозяйственные предприятия, горнодобывающая промышленность, логистические компании.




Рост предложения ВПО, как услуги, DDoS атак по найму значительно упростит появление новых групп, кроме того растет взаимодействие группировок, когда одни группировки могут использоваться на субподряде другими группировками. Некоторые группировки будут преследовать как финансовые, так и политические цели.

Текущее покрытие системами информационной безопасности АСУ ТП и Промышленного Интернета вещей оценивается в 4-6% от необходимого, что предоставляет отличные перспективы атакующим, в связи с чем в 2024 году ожидается рост количества компаний, предлагающих продукты и услуги в области ИБ АСУ ТП, рост количества патентов на тему ИБ АСУ ТП.

Защита АСУ ТП является насущной необходимостью и вопросом обеспечения функционирования предприятия и его финансовой состоятельности, а также отраслей, в том числе стратегических, и, соответственно, государств.



Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:д

-  Рассылка InfoWatch
-  ВКонтакте
-  Telegram

© InfoWatch

Полное воспроизведение, опубликование материалов запрещено.

Цитирование возможно только при указании ссылки на источник.