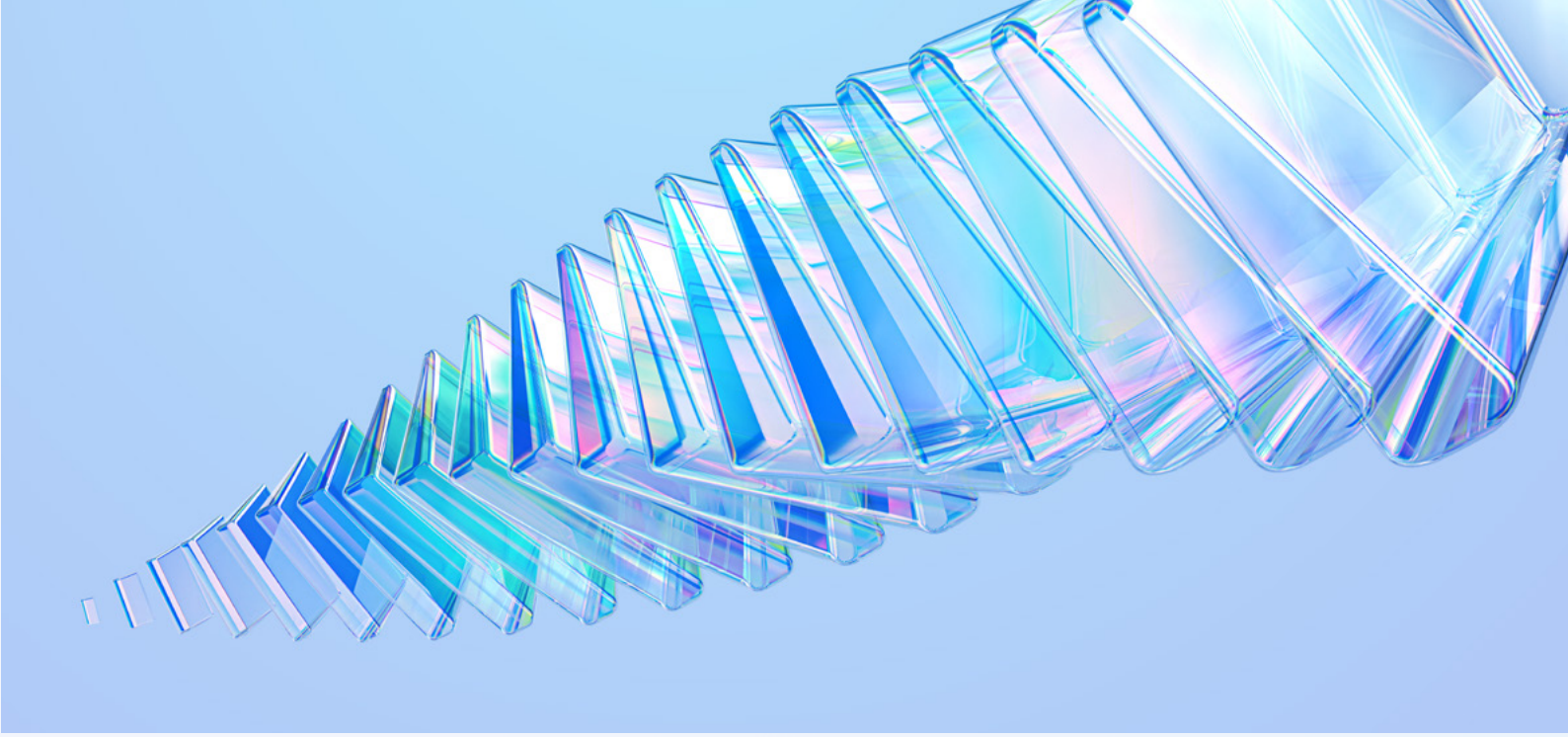
JET SECURITY TEAM

ИССЛЕДОВАНИЕ

ЗАЩИТА АСУ ТП ОТ APT-АТАК КАК ЧАСТЬ СТРАТЕГИИ КИБЕРУСТОЙЧИВОСТИ

Инфосистемы Джет
JET.SU



КЛЮЧЕВЫЕ ВЫВОДЫ

Базовые меры защиты АСУ ТП, определенные Приказами ФСТЭК России, требуют адаптации и дополнения на этапе моделирования угроз и нарушителей безопасности для эффективной защиты от APT-атак.

Формальная реализация защитных мер из базовых наборов мер в Приказах ФСТЭК России не является эффективной защитой от APT-атак.

В **45%** российских компаний промышленного сектора усредненный уровень зрелости процессов ИБ оценивается как крайне низкий (уровень зрелости по модели CMMI: «начальный[1]» или «отсутствует[2]»).

50% компаний промышленного сектора имеют низкую зрелость процессного управления ИБ на уровне всей компании.

32% предприятий промышленного сектора не реализуют ключевые процессы обеспечения ИБ в АСУ ТП (управление доступом в ИТ-инфраструктуру АСУ ТП, управление уязвимостями ИБ, мониторинг событий безопасности и управление инцидентами ИБ).

31% компаний промышленного сектора отмечают общее увеличение количества инцидентов ИБ за 2024 год.

39% компаний промышленного сектора не ведут статистику инцидентов ИБ, поскольку у них отсутствует процесс управления инцидентами ИБ.

36% компаний промышленного сектора не предъявляют требований к доступу работников подрядных организаций в свою ИТ-инфраструктуру.

86% компаний промышленного сектора не проводят эмуляции фишинговых атак и обучение для своих работников по защите от распространенных приемов социальной инженерии.

44% компаний промышленного сектора не проводят мероприятия по совершенствованию настроек безопасности компонентов АСУ ТП.

69% компаний считают шифровальщики одной из основных угроз АСУ ТП.

[1] Начальный уровень зрелости процессов управления и обеспечения ИБ характеризуется пониманием проблем и их присутствия в организации, но отсутствием стандартизованного и организованного подхода по их решению.

[2] Процессы управления и обеспечения ИБ отсутствуют.

ВВЕДЕНИЕ

В российской практике информационной безопасности (ИБ) автоматизированные системы управления технологическими процессами (АСУ ТП) уже давно входят в число приоритетных объектов защиты, так как обеспечивают функционирование критически важных предприятий, являющихся основой национальной безопасности и экономической стабильности Российской Федерации.

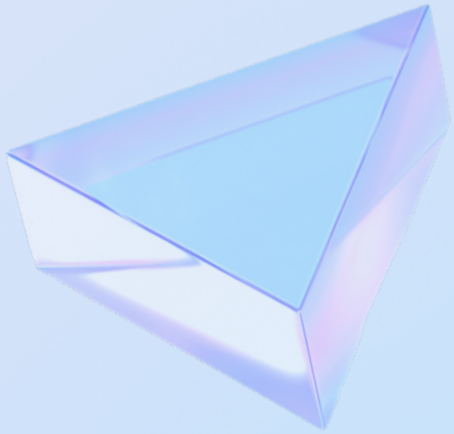
Подходы, которые используются при формировании защитных мер для таких объектов, давно определены и в большинстве случаев представляют собой следующие требования по защите.

1. Если объект защиты — **значимый объект** критической информационной инфраструктуры (КИИ), то реализуется базовый набор мер по обеспечению безопасности, определенный в соответствии с Приказом ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее — Приказ ФСТЭК №239).
2. Если объект защиты — **критически важный объект**[3], то реализуется базовый набор мер по обеспечению безопасности, определенный в соответствии с приказом ФСТЭК России от 14 марта 2014 г. №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (далее — Приказ ФСТЭК №31).
3. Если объект защиты **не попадает** под указанные нормативные требования, то реализуются меры защиты, определенные в отраслевых требованиях, или требования определяются экспертно по результатам анализа актуальных угроз.

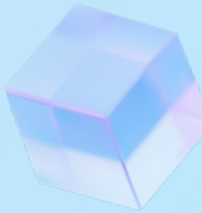
[3] Включая потенциально опасные объекты и объекты, представляющие повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Наш проектный опыт в области аудита ИБ АСУ ТП показал, что мер защиты от APT-атак недостаточно как для объектов, к которым не предъявляются требования законодательства по защите АСУ ТП, так и для тех, к которым они применяются (формальное выполнение требований приводит лишь к трате ресурсов и отсутствию реальной защищенности).

Несмотря на системность и качественную проработку базовых наборов мер защиты, упомянутые нормативно-правовые акты содержат верхнеуровневое описание защитных мер без детализации их реализации и не определяют подходы по комплексной защите от целенаправленных (APT) атак:



- Меры защиты, определенные в Приказах ФСТЭК и отраслевых требованиях, не в полном объеме определяют меры защиты и подходы по их формированию и реализации защиты от APT-атак на инфраструктуру АСУ ТП, а механизмы адаптации базового набора мер защиты не всегда эффективно применяются или не применяются вовсе.
- Моделирование угроз и нарушителей, применяемое для формирования защитных мер для АСУ ТП, редко учитывает техники, используемые APT-группировками для совершения целенаправленных атак.
- Для персонала, который эксплуатирует и защищает АСУ ТП, не проводятся специализированные киберучения по выявлению инцидентов и отработке действий в случае APT-атак. Процедуры логирования в АСУ ТП, как правило, незрелые: журналы событий хранят недостаточное количество свидетельств для проведения глубокого анализа и формирования корректирующих мер.
- В восьми из десяти предприятий промышленного сектора отсутствует регулярное обучение и проверка знаний по противодействию социальной инженерии для работников, в том числе для персонала, эксплуатирующего и защищающего АСУ ТП.



Цель отчета — предложение решений по комплексной защите АСУ ТП от APT-атак на основе экспертного опыта специалистов АО «Инфосистемы Джет». Отчет будет полезен руководителям служб ИБ и АСУ ТП, а также консультантам и экспертам в области ИБ.

При разработке отчета использовались следующие материалы:

- **Данные, полученные в ходе реализации более чем 150 проектов по обеспечению безопасности АСУ ТП специалистами АО «Инфосистемы Джет»**

- **Аналитические отчеты**
  - High-Tech Crime Trends Report 2025 от GROUP-IB
  - Киберугрозы в России и СНГ от F6

- **Аналитические отчеты и статьи по APT-группировкам**
  - Lockbit
  - Akira/Howling Scorpius:
    - профиль группировки на MITRE ATT&CK
    - отчет Trend Micro Ransomeware spotlight Akira
    - Cybersecurity Advisory от Cybersecurity and Infrastructure Security Agency
    - отчет от Unit42 (Palo Alto Networks)
  - BlackJack
  - Shadow/DarkStar/Twelve

В отчет также вошли результаты опросов ключевых заказчиков АО «Инфосистемы Джет» и внешние опросы профильной аудитории. В опросах за 2023 и 2024 годы приняли участие более 28 российских компаний, большинство которых (64%) — представители крупного бизнеса, а также средние предприятия и компании государственного сектора, имеющие более 2 тыс. работников.

ЗАЧЕМ УСИЛИВАТЬ МЕРЫ ЗАЩИТЫ АСУ ТП ОТ APT-АТАК

APT-ГРУППИРОВКИ – АКТУАЛЬНЫЕ ВНЕШНИЕ НАРУШИТЕЛИ БЕЗОПАСНОСТИ АСУ ТП

Актуальными рисками киберустойчивости АСУ ТП в Российской Федерации на текущий момент являются:

- **Массовые атаки.** Наиболее легким вариантом для злоумышленников являются атаки на доступные из сети Интернет компоненты АСУ ТП, в которых выявлены эксплуатируемые уязвимости (к примеру, атаки на программируемые логические контроллеры производства Unitronics группировкой CyberAv3ngers[4]), с политическими или идеологическими целями или массовое распространение и заражение в том числе компонентов АСУ ТП вредоносным программным обеспечением (например, шифровальщиками) для последующего вымогательства.
- **APT-атаки.** Целенаправленные атаки на промышленный сектор с целью получения финансовой выгоды для злоумышленников (APT-группировки) или нанесения максимального ущерба производственным процессам организации (хакерские группировки из недружественных государств) более затратны для злоумышленников, однако наиболее разрушительны. Текущая внешнеполитическая ситуация увеличивает количество целенаправленных атак на системообразующие предприятия в Российской Федерации.

APT-атаки представляют серьезный риск для промышленного сектора, поскольку нацелены на длительное скрытое проникновение в АСУ ТП, кражу критически важных данных и нарушение производственных процессов, которые способны привести к финансовым и репутационным потерям.

По данным, полученным из Shodan, прямой доступ к компонентам АСУ ТП не является редкостью: **1064 устройства в Российской Федерации** (помечены тегом ICS в Shodan) **имеют белые адреса в сети Интернет** и могут стать целями массовых атак

По результатам опроса ключевых заказчиков АО «Инфосистемы Джет», **более 69% компаний считают шифровальщиков** одной из основных угроз АСУ ТП

Общие мировые тенденции отмечают рост атак APT-группировок, нацеленных на приостановку деятельности промышленных предприятий. За 2023–2024 годы зафиксировано более 20 известных инцидентов ИБ, имеющих существенный финансовый ущерб, связанный с простоем производственных мощностей в результате атак

По данным отчета High-Tech Crime Trends Report 2025 от GROUP-IB, 4,8% всех APT-атак в мире в 2024 году были нацелены на промышленность, 2,2% — на транспортную отрасль и 1,9% — на энергетику, добычу газа и нефти. В промышленном секторе зафиксировано 660 APT-атак, связанных с требованием выкупа за украденные данные

[4] https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

Далее раскроем тезис о недостаточности набора технических мер защиты для выявления и предотвращения APT-атак на АСУ ТП.

1. С помощью методики профилирования угроз приоритизируем техники атак, используемые APT-группировками.
2. Для каждой техники атак определим меры защиты с использованием базы MITRE ATT&CK, которые предотвращают или снижают эффективность атак APT-группировок.
3. Оценим наличие сформированного перечня мер защиты в базовых наборах мер защиты Приказов ФСТЭК России №31 и №239.

ПОЧЕМУ БАЗОВЫХ МЕР ЗАЩИТЫ НЕДОСТАТОЧНО

В Приказах ФСТЭК №31 и №239 определены базовые меры защиты АСУ ТП, которые при должной реализации достаточны для защиты от массовых атак. Меры должны быть расширены (адаптированы) на основе результатов моделирования угроз, однако на практике мы не встречали «расширенного» набора мер защиты, учитывающего специфику целенаправленных атак, поскольку ни на законодательном, ни на отраслевом уровне не определен подход по формированию мер защиты от них. Экспертное моделирование угроз также не всегда учитывает специфику промышленных организаций и техники, используемых APT-группировками для реализации целенаправленных атак.

Для определения актуальных мер защиты от APT-атак мы рекомендуем использовать комбинацию из подходов моделирования угроз и нарушителей безопасности и профилирования угроз безопасности АСУ ТП. Моделирование угроз — давно используемый подход и описан в методике ФСТЭК России[5], в то же время профилирование угроз безопасности на практике используется крайне редко.

Профилирование угроз безопасности — это структурированный повторяемый процесс определения актуальных угроз безопасности и их приоритизация для контекста

[5] Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).

конкретной организации. В наших проектах мы используем методику профилирования угроз, основанную на методике Tidal и методе приоритизации на базе скоринга в MITRE ATT&CK Navigator[6].

В рамках профилирования угроз безопасности рассматриваются три категории потенциальных угроз:

1. **Прямые угрозы** — угрозы, реализация которых была обнаружена организацией ранее и которые потенциально могут повториться (база инцидентов ИБ, аналитика SOC и т.д.);
2. **Возможные угрозы** — потенциальные угрозы актуальные для отрасли/страны, связанные с деятельностью профессиональных преступных группировок (APT-группировки, группировки, спонсируемые недружественными организациями);
3. **Неизбирательные угрозы** — потенциальные угрозы массового характера с целью развлечения или по идеологическим соображениям, выполняемые скрипт-кидди, хактивистами, ботами.

В случае рассмотрения абстрактного промышленного предприятия мы не обладаем информацией о прямых угрозах, поэтому данные виды угроз далее не учитываются. Неизбирательные угрозы мы также не берем во внимание, поскольку они не связаны напрямую с действиями APT-группировок.

В рамках профилирования возможных угроз безопасности рассматривались следующие профессиональные преступные группировки:

- LockBit — APT-группировка, которая выполняет атаки самостоятельно и предоставляет инфраструктуру для совершения атак, нацеленных на вымогательство (Ransomware-as-a-Service, RaaS). Несмотря на то, что группировка не атакует компании из России, в 2023 году 22,22% APT-атак совершались с использованием их инструментария.
- Akira/Howling Scorpius — APT-группировка, нацеленная на SMB-предприятия, без специализации в конкретной отрасли. Входит в топ-5 наиболее активных групп, занимающихся вымогательством (более 74 атак на промышленность с марта 2023-го по октябрь 2024-го[7]).

[6] Более подробно методика профилирования угроз безопасности АСУ ТП будет представлена в нашем следующем отчете.

[7] По данным PaloAlto.

- BlackJack — проправительственная хактивистская группировка (10 атак на государственные компании Российской Федерации в 2024 году).
- Shadow/DarkStar/Twelve — APT-группировка, нацеленная на инфраструктуру и компании Российской Федерации как с целью вымогательства, так и диверсии (более 50 атак за 2024 год).

Результаты профилирования возможных угроз безопасности, сопоставление мер защиты и техник с использованием базы MITRE ATT&CK и оценка наличия соответствующих мер защиты в базовых наборах мер защиты Приказов ФСТЭК России №31 и №239 представлены в Приложении 1.

По результатам выполненной оценки можно сделать вывод, что базовые наборы мер защиты в Приказах ФСТЭК №239 и №31 не включают в себя как минимум следующие меры, необходимые для защиты от APT-атак:

- Многофакторная аутентификация учетных записей (M1032 Multi-factor Authentication):
  - Приказ ФСТЭК №31: отсутствует;
  - Приказ ФСТЭК №239: отсутствует.
- Управление действиями привилегированных учетных записей (M1026 Privileged Account Management):
  - Приказ ФСТЭК №31: АУД.9 «Анализ действий пользователей», только для первого класса защищенности;
  - Приказ ФСТЭК №239: АУД.9 «Анализ действий пользователей», только для первой категории значимости.
- Поведенческий анализ файлов в виртуальной изолированной среде (M1048 Application Isolation and Sandboxing):
  - Приказ ФСТЭК №31: ЗИС.7 «Использование эмулятора среды функционирования программного обеспечения («песочница»)», не является обязательным;
  - Приказ ФСТЭК №239: ЗИС.7 «Использование эмулятора среды функционирования программного обеспечения («песочница»)», не является обязательным.
- Обнаружение и предотвращение вторжений (M1031 Network Intrusion Prevention, M1050 Exploit Protection:
  - Приказ ФСТЭК №31: СОВ.1 «Обнаружение и предотвращение компьютерных атак», только для первого и второго класса защищенности;

- Приказ ФСТЭК №239: СОВ.1 «Обнаружение и предотвращение компьютерных атак», только для первой и второй категории значимости.

- Отслеживание угроз ИБ и автоматизация обработки Threat Intelligence данных (M1019 Threat Intelligence Program):
  - Приказ ФСТЭК №31: отсутствует;
  - Приказ ФСТЭК №239: отсутствует.
- Анализ поведения и адаптивного контроля аномалий на компонентах АСУ ТП (M1040 Behavior Prevention on Endpoint, M1038 Execution Prevention):
  - Приказ ФСТЭК №31: частично покрывается мерой защиты АВЗ.3 «Контроль использования архивных, исполняемых и зашифрованных файлов» и ОПС.1 «Управление запуском (обращениями) компонентов программного обеспечения», только для первого класса защищенности;
  - Приказ ФСТЭК №239: частично покрывается мерой защиты АВЗ.3 «Контроль использования архивных, исполняемых и зашифрованных файлов» и ОПС.1 «Управление запуском (обращениями) компонентов программного обеспечения», только для первой категории значимости.
- Совершенствование настроек безопасности операционных систем, прикладного программного обеспечения и инфраструктурных сервисов (M1028 Operating System Configuration, M1042 Disable or Remove Feature or Program, M1015 Active Directory Configuration):
  - Приказ ФСТЭК №31: явно не определено, п. 16.7 и п. 16.8 можно рассматривать как частичную реализацию;
  - Приказ ФСТЭК №239: явно не определено, п. 11.2 и п. 13.4 можно рассматривать как частичную реализацию.
- Контроль утечек защищаемой информации (M1057 Data Loss Prevention):
  - Приказ ФСТЭК №31: ЗИС.17 «Защита информации от утечек», не является обязательным;
  - Приказ ФСТЭК №239: ЗИС.17 «Защита информации от утечек», не является обязательным.

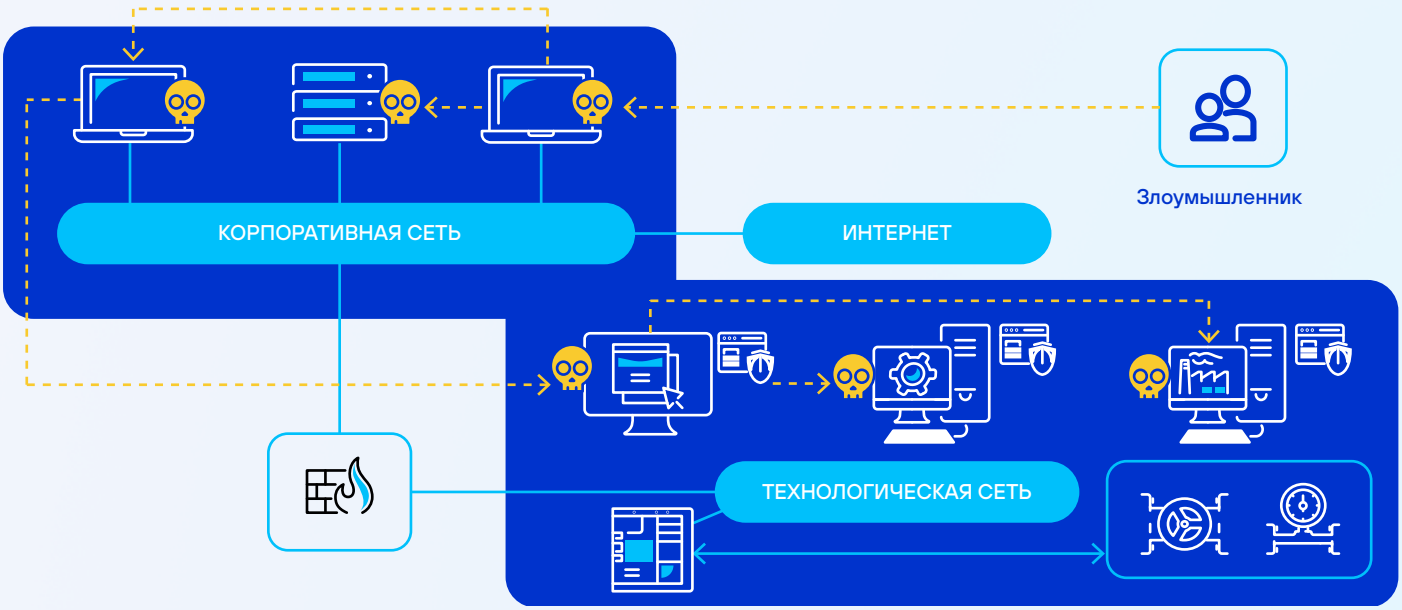
- Контроль зашифрованного трафика (M1020 SSL/TLS Inspection):
  - Приказ ФСТЭК №31: явно не определен контроль зашифрованного трафика, АУД.5 «Контроль и анализ сетевого трафика» можно рассматривать как частичную реализацию;
  - Приказ ФСТЭК №239: явно не определен контроль зашифрованного трафика, АУД.5 «Контроль и анализ сетевого трафика» можно рассматривать как частичную реализацию.

Далее на нескольких типовых сценариях развития целенаправленных атак рассмотрим, какие из указанных мер защиты помогут затруднить или предотвратить действия потенциального нарушителя. Дополнительно приведем практические кейсы из нашей проектной практики (аудиты защищенности АСУ ТП и киберкриминалистика), подтверждающие актуальность указанных сценариев, и оценим наличие указанных средств защиты информации в базовых наборах мер защиты в Приказах ФСТЭК России №31 и №239.

ТИПОВЫЕ СЦЕНАРИИ APT-АТАК И ЗАЩИТНЫЕ МЕРЫ

Атака через корпоративный сегмент

Наиболее частой разновидностью APT-атак являются атаки с проникновением злоумышленника через корпоративный сегмент сети передачи данных посредством фишинга или социальной инженерии.



Получение доступа злоумышленником в корпоративный сегмент является начальной точкой атаки. После повышения привилегий и изучения активов предприятия происходит развитие атаки и обнаружение других сегментов сети, в том числе технологических. После закрепления в инфраструктуре АСУ ТП и эксфильтрации критичных данных злоумышленники, как правило, требуют выкуп за похищенные данные или шифруют компоненты верхнего уровня АСУ ТП (серверы АСУ ТП, АРМ операторов и инженерные станции) и серверы критичных инфраструктурных сервисов (серверы резервного копирования), чтобы потребовать выкуп за передачу ключа дешифрования данных.

КЕЙС №1

«Бумага все стерпит»

Специалистами киберкриминалистики «Инфосистемы Джет» проводились работы по исследованию и устранению последствий атаки на предприятие в сфере обрабатывающей промышленности.

По результатам исследования выяснилось, что злоумышленники использовали классическую схему — массовый фишинг, компрометацию учетных записей пользователей, поиск на периметре ИТ-инфраструктуры предприятия сервисов удаленного доступа (RDP), использование данного сервиса для доступа к рабочим местам пользователей посредством скомпрометированных учетных записей, а далее закрепление и повышение привилегий.

Активная фаза распространения в корпоративной сети началась **спустя два года после получения изначального доступа** (возможно, это связано с перепродажей изначального доступа в ИТ-инфраструктуру).

Атака не затронула производственный сегмент предприятия, поскольку было выявлено развитие атаки — перемещение злоумышленников по ИТ-инфраструктуре и несанкционированное использование привилегированных учетных записей. Это позволило остановить дальнейшее продвижение злоумышленников и оперативно закрыть удаленный доступ через RDP.

Актуальные меры защиты[8]

Основные меры для замедления/остановки развития APT-атаки из корпоративного в технологический сегмент сети передачи данных, сформированные на основе нашего проектного опыта по защите АСУ ТП, представлены в таблице ниже.

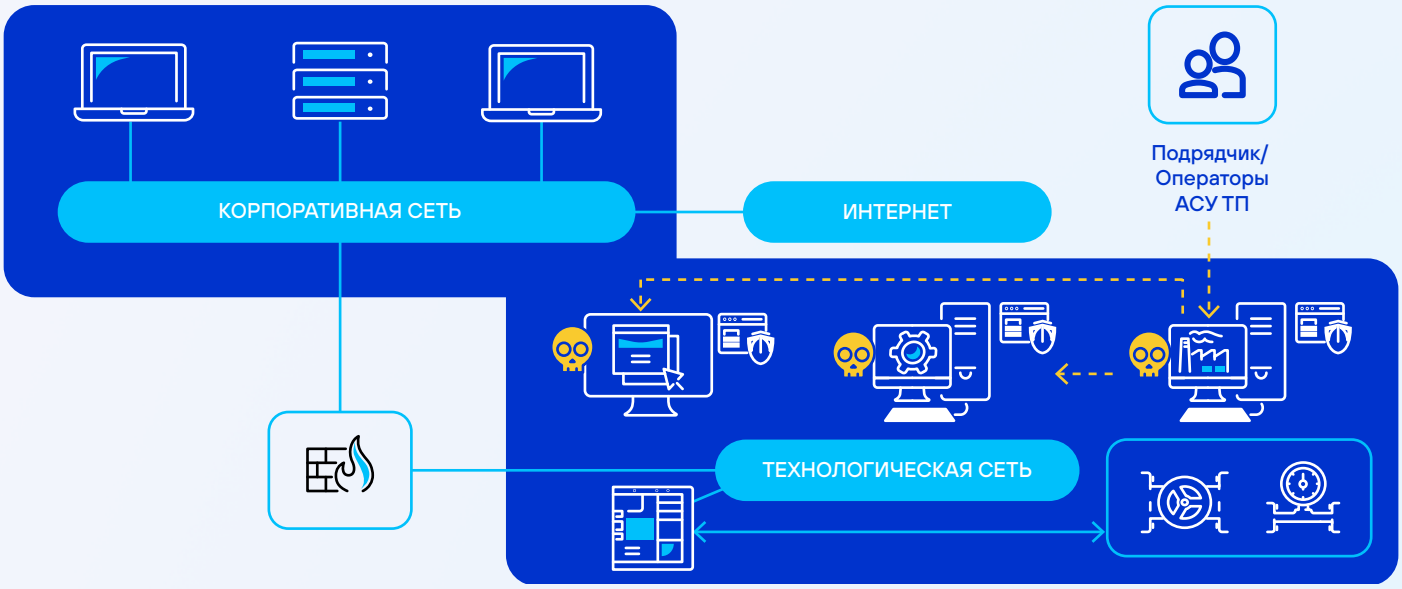
[8] Сформированы по рекомендациям в рамках аудитов ИБ АСУ ТП или результатам проектирования систем обеспечения ИБ АСУ ТП.

Мера защиты информации	Решаемые задачи	Наличие в базовом наборе мер Приказа №239	Наличие в базовом наборе мер Приказа №31
Сегментация технологического сегмента / изоляция технологического сегмента (физическая или с применением однонаправленных шлюзов)	Ограничение возможности влияния на компоненты АСУ ТП из корпоративного сегмента, затруднение развития вектора атаки в технологический сегмент	ЗИС.4 (только 1-я и 2-я категории значимости)	ЗИС.4 (только 1-й и 2-й классы защищенности)
Межсетевое экранирование на уровне периметра технологического сегмента	Управление сетевыми потоками в технологический сегмент, ограничение возможности влияния на компоненты АСУ ТП из корпоративного сегмента	ЗИС.2, ЗИС.6, ЗИС.35	ЗИС.2, ЗИС.6 (необязательный), ЗИС.35 (только 1-й и 2-й классы защищенности)
Обнаружение или предотвращение вторжений на уровне периметра технологического сегмента	Выявление и блокирование сетевых атак на периметр технологического сегмента	СОВ.1 (только 1-я и 2-я категории значимости)	СОВ.1 (только 1-й и 2-й классы защищенности)
Реализация DMZ-сегмента АСУ ТП — буферной зоны для взаимодействия корпоративных систем (с MES-системой, OPC-серверами или серверами отчетности)	Ограничение числа доступных сервисов технологического сегмента для развития атаки из корпоративного сегмента	ЗИС.5	ЗИС.5
Антивирусная защита компонентов АСУ ТП	Выявление распространения вредоносного кода	АВЗ.1	АВЗ.1
Анализ поведения и адаптивного контроля аномалий на компонентах АСУ ТП	Выявление применения несанкционированного воздействия на компоненты АСУ ТП	–	–
Анализ уязвимостей периметра технологического сегмента	Устранение известных уязвимостей периметра технологического сегмента для снижения возможностей развития атаки из корпоративного сегмента	АУД.2	АУД.2
Управление действиями привилегированных учетных записей при доступе в технологический сегмент (PIM/PAM)	Единая точка входа и контроль действий привилегированных учетных записей в технологическом сегменте	АУД.9 (только 1-я категория значимости)	АУД.9 (только 1-й класс защищенности)
Контроль утечек защищаемой информации (DLP)	Выявление несанкционированного обмена данными	ЗИС.17 (необязательный)	ЗИС.17 (необязательный)
Применение двухфакторной аутентификации для привилегированных учетных записей на компонентах периметра технологического сегмента	Усиленная аутентификация для привилегированных учетных записей на компонентах периметра технологического сегмента	–	–

Отслеживание угроз ИБ и автоматизация обработки Threat Intelligence (TI) данных	Обработка TI-данных, выгрузка индикаторов компрометации на другие средства защиты информации, автоматизация ретроспективного и проактивного поиска индикаторов компрометации в событиях SIEM	–	–
Централизованный мониторинг событий безопасности и реагирование на инциденты ИБ (SIEM и SOAR)	Выявление признаков атаки, информирование ответственных лиц и ускорение реагирования на инцидент ИБ	АУД.7, ИНЦ.1, ИНЦ.2, ИНЦ.3	АУД.7, ИНЦ.1, ИНЦ.2, ИНЦ.3

АТАКА ЧЕРЕЗ УДАЛЕННЫЕ РАБОЧИЕ МЕСТА

Другой разновидностью APT-атаки является компрометация APT-группировкой рабочих мест работников предприятия или работников подрядчика, имеющих удаленный доступ в технологический сегмент предприятия. Такие атаки могут происходить как в рамках эксплуатации систем, так и в рамках технологических окон обслуживания.



Операторы или инженеры АСУ ТП, имеющие доступ к компонентам АСУ ТП, могут случайно или целенаправленно внедрить вредоносное ПО и организовать несанкционированное удаленное подключение для удобства эксплуатации АСУ ТП, которое может также использовать злоумышленник для доступа в инфраструктуру АСУ ТП. Подрядчик имеет аналогичные возможности в рамках обслуживания или модернизации АСУ ТП. Например, он может оставить небольшой роутер с выходом в сеть Интернет, через который он выполнял сервисные работы по обслуживанию или осуществлял удаленную поддержку «по дружбе».

КЕЙС №2

«Поддержка 24/7 любой ценой»

В периметре технологического сегмента компании из сферы пищевой промышленности в рамках аудита ИБ АСУ ТП мы обнаружили недостатки, которые могли привести к указанному сценарию атаки:

- **Наличие элементов Shadow IT**: 3G/4G-модемов, подключенных непосредственно к серверам АСУ ТП и используемых подрядчиком для оперативного доступа к компонентам АСУ ТП (знали об этом только инженеры АСУ ТП). Контроль подключений к инфраструктуре АСУ ТП, ведение записей сессий, мониторинг аномальной активности на серверах АСУ ТП не осуществлялись. Помимо этого, 3G/4G-модемы, несогласованные с подразделением ИБ, были подключены к инженерным АРМ АСУ ТП для оперативного доступа инженеров во внерабочее время из дома.
- **Наличие ПО удаленного доступа (TeamViewer/Anydesk) на инженерных АРМ**, используемых для оперативного доступа инженеров во внерабочее время из дома. Подразделение ИБ не знало о наличии данного ПО в инфраструктуре АСУ ТП. Защитные меры для контроля использования такого канала доступа и защиты удаленных рабочих мест инженеров АСУ ТП отсутствовали.
- **Наличие уязвимостей во внешних сервисах подрядчика** (корпоративный портал, почтовая система, IP-телефония и т.д.), имеющих дату публикации более трех лет назад и публичные эксплойты. Уязвимости были выявлены в рамках работ по киберразведке и косвенно подтвердили низкую зрелость процесса управления уязвимостями в ИТ-инфраструктуре данного подрядчика.

Актуальные меры защиты

Основные меры для замедления/остановки развития APT-атаки на АСУ ТП через подрядчика/санкционированного удаленного пользователя, сформированные на основе нашего проектного опыта по защите АСУ ТП, представлены в таблице ниже.

Мера защиты информации	Решаемые задачи	Наличие в базовом наборе мер Приказа №239	Наличие в базовом наборе мер Приказа №31
Инвентаризация и оперативный контроль устройств в технологической сети, контроль сетевых подключений (Port Security, NAC и др.)	Выявление/предотвращение несанкционированных подключений в технологическом сегменте	ИАФ.2[9]	ИАФ.2[9]
Управление действиями привилегированных учетных записей при доступе в технологический сегмент (PIM/PAM)	Единая точка входа и контроль действий привилегированных учетных записей в технологическом сегменте	АУД.9 (только 1-я категория значимости)	АУД.9 (только 1-й класс защищенности)
Применение двухфакторной аутентификации для привилегированных учетных записей на компонентах АСУ ТП	Усиленная аутентификация для привилегированных учетных записей на компонентах АСУ ТП	–	–

[9] В большинстве обследованных АСУ ТП реализуется только для управления устройствами на уровне хостов, а не на уровне сети.

Мониторинг сетевого трафика и выявление аномалий (NTA)	Контроль сетевого трафика внутри технологического сегмента и выявление несанкционированных действий и признаков атаки	АУД.5 (только 1-я категория значимости)	АУД.5 (только 1-й класс защищенности)
Межсетевое экранирование на уровне технологической сети	Ограничение сетевого доступа подрядчика только сегментами, в которых проводятся работы, затруднение развития вектора атаки в технологическом сегменте	ЗИС.6, ЗИС.35	ЗИС.6 (необязательный), ЗИС.35 (только 1-й и 2-й классы защищенности)
Антивирусная защита компонентов АСУ ТП	Выявление распространения вредоносного кода	АВЗ.1	АВЗ.1
Анализ поведения и адаптивного контроля аномалий на компонентах АСУ ТП	Выявление применения несанкционированного воздействия на компоненты АСУ ТП	–	–
Анализ уязвимостей компонентов АСУ ТП	Устранение известных уязвимостей компонентов АСУ ТП для снижения возможностей развития атаки	АУД.2	АУД.2
Отслеживание угроз ИБ и автоматизация обработки Threat Intelligence (TI) данных	Обработка TI-данных, выгрузка индикаторов компрометации на другие средства защиты информации, автоматизация ретроспективного и проактивного поиска индикаторов компрометации в событиях SIEM	–	–
Централизованный мониторинг событий безопасности и реагирование на инциденты ИБ (SIEM и SOAR)	Выявление признаков атаки, информирование ответственных лиц и ускорение реагирования на инцидент ИБ	АУД.7, ИНЦ.1, ИНЦ.2, ИНЦ,3	АУД.7, ИНЦ.1, ИНЦ.2, ИНЦ,3

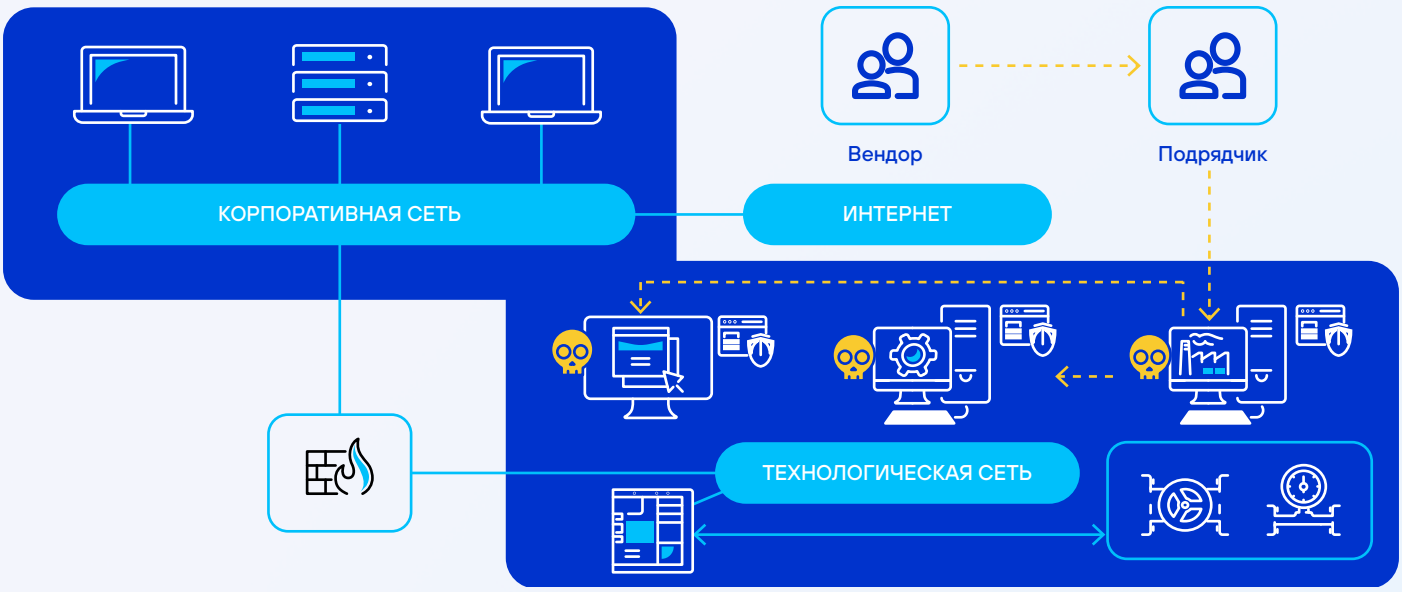
АТАКА ЧЕРЕЗ ЦЕПОЧКУ ПОСТАВОК

Третий тип атаки совмещает в себе цепочку участников:

- производителя, который выпускает обновления для компонентов АСУ ТП;
- подрядчика, осуществляющего обслуживание компонентов АСУ ТП.

Компрометация производителя компонентов АСУ ТП (например, SCADA-систем) может привести к распространению обновлений или версий компонентов АСУ ТП, имеющих вредоносное ПО, активируемое при определенных условиях. Компрометация ИТ-инфраструктуры подрядчика, осуществляющего сервисное обслуживание/модерниза-

цию АСУ ТП, может привести к тем же последствиям. Такие атаки наиболее опасны, так как обнаружить вредоносное ПО намного сложнее — по умолчанию доверяют производителю АСУ ТП и подрядчику, выполняющему работы.



В данной ситуации наилучшим решением будет выбор проверенных вендоров и поставщиков решений. Но даже это не спасает от возможной компрометации системы, поскольку всегда остается человеческий фактор (социальная инженерия в отношении подрядчика/вендора) и наличие недостатков обеспечения ИБ в ИТ-инфраструктуре вендора или поставщика решений.

Практические кейсы по данному сценарию встречаются редко, наиболее известны кейсы Stuxnet[10] и Industroyer[11].

АКТУАЛЬНЫЕ МЕРЫ ЗАЩИТЫ

Основным направлением предотвращения APT-атаки с использованием несанкционированно измененных обновлений, версий ПО через производителя/подрядчика представлены в таблице ниже.

[10] https://securelist.ru/stuxnet-pervye-zhertvy/24277/

[11] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

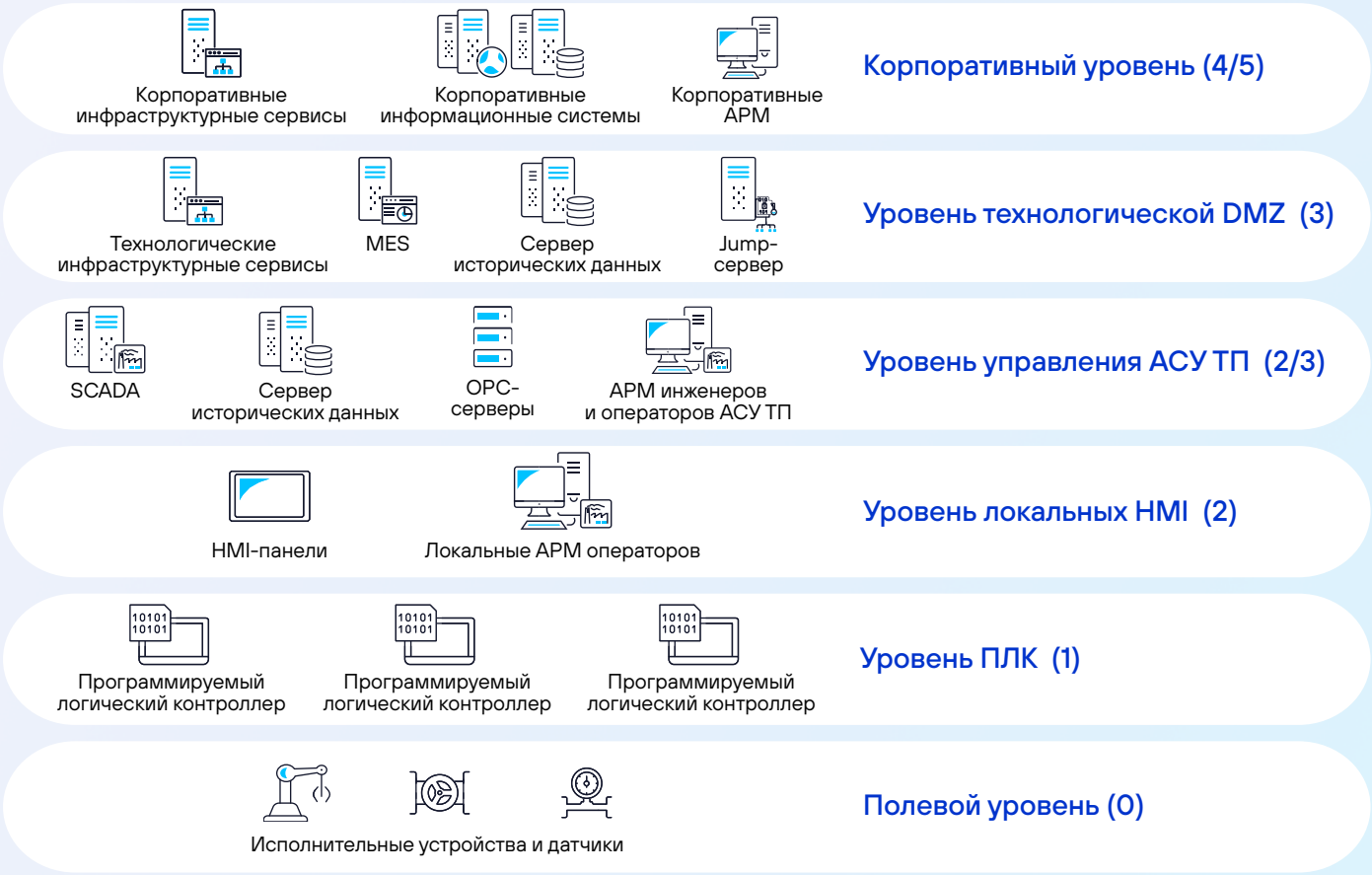
Мера защиты информации	Решаемые задачи	Наличие в базовом наборе мер Приказа №239	Наличие в базовом наборе мер Приказа №31
Выбор проверенных производителей и поставщиков решений АСУ ТП (проверяемых в том числе внешними аудиторами ИБ)	Оценка защищенности поставщиков услуг	–	–
Использование производителями АСУ ТП инструментов безопасной разработки ПО и контроль на всех этапах разработки и поставки ПО	Затруднение реализации вектора атаки на АСУ ТП	–[12]	–
Поведенческий анализ файлов в виртуальной изолированной среде (использующих в том числе проверки с манипуляцией временем)	Выявление аномалий в обновлениях компонентов АСУ ТП и других файлах, получаемых от производителей и поставщиков решений АСУ ТП	ЗИС.7 (необязательно для всех категорий значимости)	ЗИС.7 (необязательно для всех классов защищенности)
Мониторинг сетевого трафика и выявление аномалий (NTA)	Контроль сетевого трафика внутри технологического сегмента и выявление несанкционированных действий и признаков атаки	АУД.5 (только 1-я категория значимости)	АУД.5 (только 1-я категория значимости)
Антивирусная защита компонентов АСУ ТП	Выявление распространения вредоносного кода	АВЗ.1	АВЗ.1
Анализ поведения и адаптивного контроля аномалий на компонентах АСУ ТП	Выявление применения несанкционированного воздействия на компоненты АСУ ТП	–	–
Анализ уязвимостей компонентов АСУ ТП	Устранение известных уязвимостей компонентов АСУ ТП для снижения возможностей развития атаки	АУД.2	АУД.2
Отслеживание угроз ИБ и автоматизация обработки Threat Intelligence (TI) данных	Обработка TI-данных, выгрузка индикаторов компрометации на другие средства защиты информации, автоматизация ретроспективного и проактивного поиска индикаторов компрометации в событиях SIEM	–	–
Централизованный мониторинг событий безопасности и реагирование на инциденты ИБ (SIEM и SOAR)	Выявление признаков атаки, информирование ответственных лиц и ускорение реагирования на инцидент ИБ	АУД.7, ИНЦ.1, ИНЦ.2, ИНЦ,3	АУД.7, ИНЦ.1, ИНЦ.2, ИНЦ,3

[12] Частично данные меры защиты реализуются требованиями Приказа ФСТЭК №239 в п. 29.3.

РЕКОМЕНДАЦИИ ПО УСИЛЕНИЮ МЕР ЗАЩИТЫ АСУ ТП ОТ APT-АТАК

Для построения системы обеспечения ИБ АСУ ТП в центре информационной безопасности «Инфосистемы Джет» применяется стратегия киберустойчивости АСУ ТП, при формировании которой мы опирались в том числе на результаты профилирования угроз для АСУ ТП в части определения защитных мер, необходимых для защиты от APT-атак. Такой подход по защите АСУ ТП адаптируется в каждом случае под организационную и технологическую структуры защищаемого предприятия с учетом профилирования угроз безопасности, актуальных для данной отрасли.

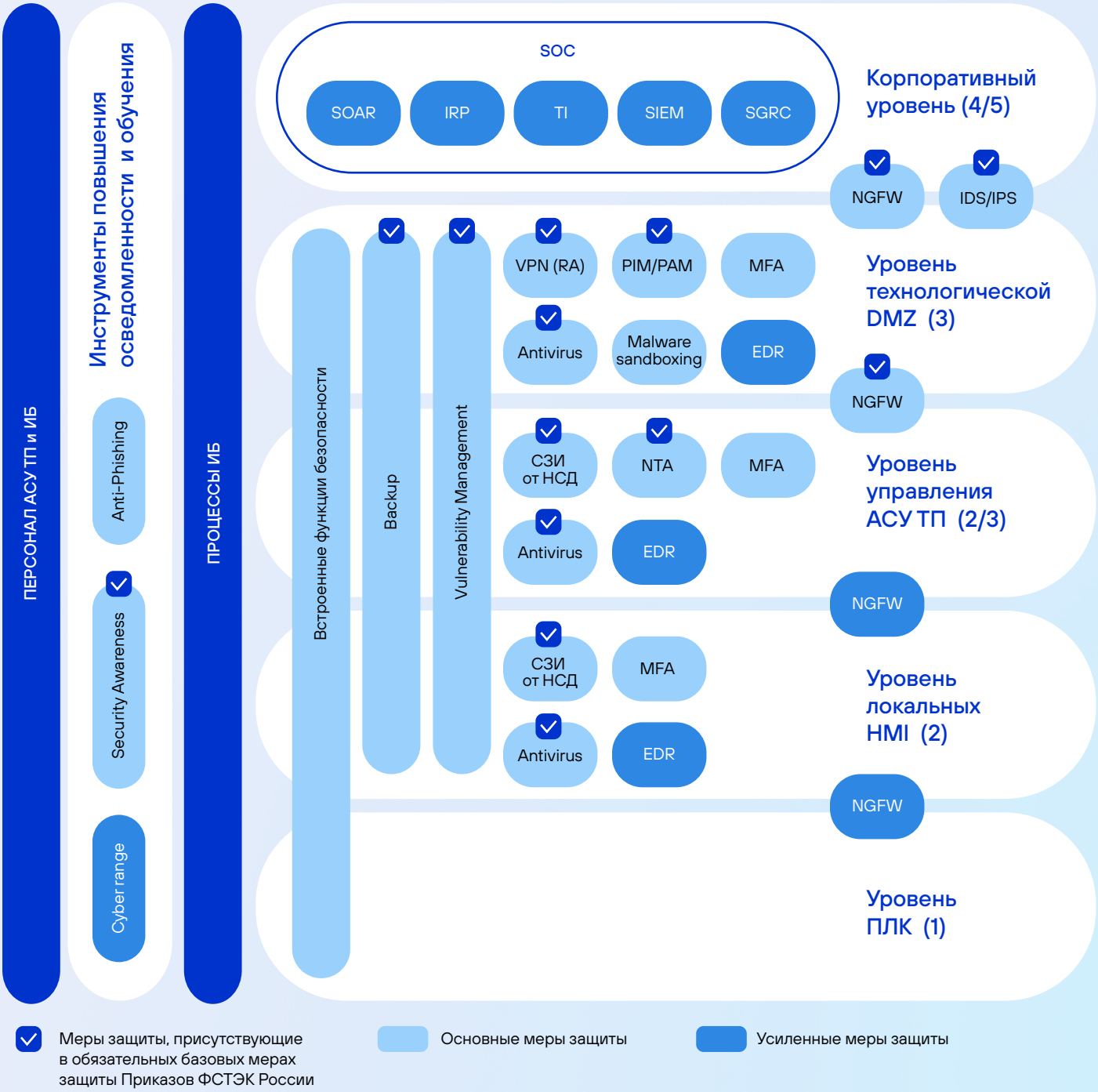
Для унификации подхода по защите АСУ ТП мы рассматриваем адаптированную референсную модель Пердью[13], представленную на схеме ниже.



[13] Модель Пердью (Purdue Enterprise Reference Architecture, PERA) — это референсная архитектура промышленного предприятия, которая описывает основные уровни автоматизации и процессы в технологическом секторе.

В качестве объектов защиты рассматриваются компоненты АСУ ТП, расположенные на уровнях 1–3, поскольку остальные уровни или не содержат интеллектуальных устройств (не рассматриваются интеллектуальные сенсоры/устройства с интеллектуальными граничными вычислениями/IoT-устройства, так как они на данный момент редко используются в промышленном секторе РФ) или требуют отдельной проработки комплекса защитных мер (корпоративный уровень, ИТ-инфраструктура).

Распределение защитных мер по уровням референсной модели АСУ ТП в соответствии с нашим подходом представлено на схеме ниже.



Важно отметить, что данный подход содержит не только набор технических мер защиты, но и комплекс процессов управления и обеспечения ИБ, распределенных по доменам:

1. Стратегическое обеспечение ИБ АСУ ТП:

- Управление ИБ АСУ ТП: определение стратегии развития ИБ АСУ ТП и организационно-штатной структуры для обеспечения ИБ АСУ ТП в соответствии с требованиями законодательства по защите КИИ (роли, задачи по обеспечению ИБ и отчетности), работа с несоответствиями и улучшениями по обеспечению ИБ.
- Методология и управление внутренними нормативными документами, регламентирующими процессы обеспечения ИБ АСУ ТП.
- Контроль соответствия регуляторным требованиям по защите АСУ ТП: отслеживание изменений законодательства, оценка выполнения требований законодательства, выполнение корректирующих мероприятий.
- Управление рисками ИБ АСУ ТП: моделирование угроз и нарушителя безопасности, оценка и приоритизация рисков ИБ АСУ ТП, обработка рисков ИБ АСУ ТП.

2. Оперативное обеспечение ИБ АСУ ТП:

- Управление доступом в ИТ-инфраструктуру АСУ ТП: управление идентификаторами и аутентификаторами пользователей, управление правами доступа, усиленная аутентификация привилегированных пользователей, использование защищенных протоколов доступа к компонентам АСУ ТП, управление доступом внешних пользователей и т.д.
- Защита сетевой инфраструктуры АСУ ТП: защита сетевого периметра технологической сети, организация сегментации и контроля сетевых потоков между сегментами технологической сети, обнаружение и предотвращение вторжений на уровне сети, выявление аномалий в сетевом трафике, совершенствование настроек безопасности сетевого оборудования.
- Защита системной инфраструктуры АСУ ТП: совершенствование настроек безопасности серверов, АРМ и ПЛК, антивирусная защита компонентов АСУ ТП, обнаружение сложных и целевых атак на компоненты АСУ ТП, контроль использования съемных носителей, ограничение разрешенного к установке ПО и т.д.

- Защита приложений: безопасная разработка ПО АСУ ТП (SCADA, DCS, MES-систем), контроль на всех этапах разработки и поставки ПО, совершенствование настроек прикладного ПО, безопасные интеграционные механизмы с внешними системами.
- Управление уязвимостями ИБ: проведение сканирований защищенности компонентов АСУ ТП, устранение выявленных уязвимостей, мониторинг уязвимостей с использованием открытых источников.
- Физическая безопасность АСУ ТП: контроль физического доступа к компонентам АСУ ТП и съемным носителям, видеонаблюдение.
- Мониторинг событий безопасности и управление инцидентами ИБ: регистрация событий безопасности и их централизованное хранение, синхронизация точного времени, выявление, категорирование и реагирование на инциденты ИБ, устранение последствий инцидентов ИБ.
- Обеспечение непрерывности функционирования АСУ ТП: определение параметров непрерывности АСУ ТП, оценка рисков непрерывности деятельности, разработка и тестирование планов аварийного восстановления, мониторинг безотказного функционирования, резервное копирование данных и тестирование возможности восстановления из резервных копий и т.д.
- Обеспечение ИБ при взаимодействии с подрядчиками (внешними сторонами): оценка безопасности внешних организаций (подрядчиков), осуществляющих доступ к компонентам АСУ ТП, организация безопасного доступа внешних организаций к компонентам АСУ ТП, проверка файлов, получаемых от внешних организаций, на наличие вредоносного кода, мониторинг действий пользователей внешних организаций, ведение реестра подрядчиков, блокировка доступа пользователей внешних организаций и другие проверки по завершении работ.
- Повышение осведомленности персонала: обучение по защите АСУ ТП и тестирование знаний работников, ответственных за эксплуатацию и защиту АСУ ТП (в том числе подрядчиков), тестирования на проникновение с использованием методов социальной инженерии (в том числе учебные фишинговые атаки на инженерный персонал), проведение киберучений и реализация киберполигона.

Реализация защитных мер по указанным доменам позволяет защитить АСУ ТП от большинства APT-атак, поскольку реализует необходимые процессы управления и обеспечения ИБ и ключевые средства защиты информации, которые существенно замедлят или предотвратят реализацию техник, применяемых APT-группировками.

ЗАКЛЮЧЕНИЕ

Современный уровень киберугроз заставляет смотреть на обеспечение защиты АСУ ТП шире, чем просто выполнение обязательных требований законодательства по их защите, опираться на лучшие практики и в ряде случаев применять нестандартные подходы в реализации уже известных мер защиты. Специфика АСУ ТП диктует свои требования и ограничения по реализации классических подходов защиты и требует особого подхода в формировании альтернативных мер защиты и компенсирующих мер.

По результатам нашего опроса, более 50% предприятий промышленного сектора имеют низкую зрелость процессного управления ИБ на уровне всего предприятия, а 32% предприятий не реализуют ключевые процессы обеспечения ИБ в АСУ ТП (управление доступом в ИТ-инфраструктуру АСУ ТП, управление уязвимостями ИБ, мониторинг событий безопасности и управление инцидентами ИБ).

Такая неутешительная картина свидетельствует о том, что начинать защиту АСУ ТП нужно с донесения важности процессного подхода в обеспечении ИБ. Наличие даже самых совершенных технических мер защиты без функционирующих организационных мер, обученного персонала не является панацеей и даст лишь ложное ощущение спокойствия. Иллюзия безопасности может привести к катастрофическим последствиям, особенно в АСУ ТП, где последствия от инцидентов ИБ — это зачастую нарушение работы опасных производственных объектов и ущерб жизни и здоровью обслуживающего персонала.

ПРИЛОЖЕНИЕ

Результаты профилирования возможных угроз безопасности определили приоритизированные техники MITRE ATT&CK, которые наиболее часто используют указанные преступные группировки[14]:

1. **Initial Access:**
   - 1.1. T1190: Exploit Public-Facing Application
   - 1.2. T1133: External Remote Service
   - 1.3. T1078: Valid Accounts
   - 1.4. T1566: Phishing
   - 1.5. T1199: Trusted Relationship
   - 1.6. T1189: Drive-by Compromise
2. **Execution:**
   - 2.1. T1059: Command and Scripting Interpreter
   - 2.2. T1569.002: System Services: Service Execution
   - 2.3. T1053: Scheduled Task/Job
   - 2.4. T1106: Native API
   - 2.5. T1047: Windows Management: Instrumentation
   - 2.6. T1204.002: User Execution: Malicious File
   - 2.7. T1072: Software Deployment Tools
3. **Persistence:**
   - 3.1. T1078.002: Valid Accounts: Domain Accounts
   - 3.2. T1136.002: Create Account: Domain Account
   - 3.3. T1133: External Remote Service
   - 3.4. T1547.001: Boot or Logon Autostart Execution: Registry Run Keys
   - 3.5. T1136.001: Create Account: Local Account
   - 3.6. T1053.005: Scheduled Task/Job: Scheduled Task
   - 3.7. T1543.003: Create or Modify System Process: Windows Service
   - 3.8. T1574.006: Hijack Execution Flow: Dynamic Linker Hijacking
   - 3.9. T1505.003: Server Software Component: Web Shell

[14] На основе аналитических отчетов и аналитики, указанных во введении, которые описывают техники атак, ранее проведенные группировками.

4. **Privilege Escalation:**
    - 4.1. T1078.002: Valid Accounts: Domain Accounts
    - 4.2. T1078.003: Valid Accounts: Local Accounts
    - 4.3. T1068: Exploitation for Privilege Escalation
    - 4.4. T1053.005: Scheduled Task/Job: Scheduled Task
    - 4.5. T1543.003: Create or Modify System Process: Windows Service
    - 4.6. T1548: Abuse Elevation Control Mechanism
    - 4.7. T1547: Boot or Logon Autostart Execution
    - 4.8. T1484.001: Domain Policy Modification: Group Policy Modification
5. **Defense Evasion:**
    - 5.1. T1562.001: Impair Defenses: Disable or Modify Tools
    - 5.2. T1078.002: Valid Accounts: Domain Accounts
    - 5.3. T1070.001: Indicator Removal: Clear Windows Event Logs
    - 5.4. T1070.004: Indicator Removal on Host: File
    - 5.5. T1036.004: Masquerading: Masquerade Task or Service
    - 5.6. T1036.005: Masquerading: Match Legitimate Name or Location
    - 5.7. T1484.001: Domain Policy Modification: Group Policy Modification
    - 5.8. T1112: Modify Registry
    - 5.9. T1550.002: Use Alternate Authentication Material: Pass the Hash
    - 5.10. T1562.004: Impair Defenses: Disable or Modify System Firewall
    - 5.11. T1620: Reflective Code Loading
    - 5.12. T1027: Obfuscated Files or Information
    - 5.13. T1480.001: Execution Guardrails: Environmental Keying
6. **Credential Access:**
    - 6.1. T1003.001: OS Credential Dumping: LSASS Memory
    - 6.2. T1555.003: Credentials from Password Stores: Credentials from Web Browsers
    - 6.3. T1555.004: Credentials from Password Stores: Windows Credential Manager
    - 6.4. T1555.005: Credentials from Password Stores: Password Managers
    - 6.5. T1003.003: OS Credential Dumping: NTDS
    - 6.6. T1003.006: OS Credential Dumping: DCSync
    - 6.7. T1552.001: Unsecured Credentials: Credentials in Files

6.8. T1552.003: Unsecured Credentials: Bash History

6.9. T1110: Brute Force

6.10. T1003: OS Credential Dumping

7. Discovery:

7.1. T1082: System Information Discovery

7.2. T1069.001: Permission Groups Discovery: Local Groups

7.3. T1069.002: Permission Groups Discovery: Domain Groups

7.4. T1482: Domain Trust Discovery

7.5. T1018: Remote System Discovery

7.6. T1046: Network Service Discovery

7.7. T1057: Process Discovery

7.8. T1087.001: Account Discovery: Local Account

7.9. T1087.002: Account Discovery: Domain Account

7.10. T1518: Software Discovery

7.11. T1033: System Owner/User Discovery

7.12. T1016.001: System Network Configuration Discovery: Internet Connection Discovery

7.13. T1049: System Network Connections Discovery

7.14. T1083: File and Directory Discovery

7.15. T1135: Network Share Discovery

7.16. T1654: Log Enumeration

7.17. T1614.001: System Location Discovery: System Language Discovery

8. Lateral Movement:

8.1. T1570: Lateral Tool Transfer

8.2. T1021.001: Remote Services: Remote Desktop Protocol

8.3. T1021.002: Remote Services: SMB/Windows Admin Shares

8.4. T1021.006: Remote Services: Windows Remote Management

8.5. T1210: Exploitation of Remote Services

8.6. T1550.002: Use Alternate Authentication Material: Pass the Hash

8.7. T1021.003: Remote Services: DCOM (Distributed Component Object Model)

8.8. T1021.004: Remote Services: SSH

9. **Collection:**
    - 9.1. T1560.001: Archive Collected Data: Archive via Utility
    - 9.2. T1005: Data from Local System
    - 9.3. T1039: Data from Network Shared Drive
    - 9.4. T1213: Data from Information Repositories
10. **Command and Control:**
    - 10.1. T1219: Remote Access Software
    - 10.2. T1071.001: Application Layer Protocol: Web Protocols
    - 10.3. T1572: Protocol Tunneling
    - 10.4. T1132.001: Data Encoding: Standard Encoding
    - 10.5. T1132.002: Data Encoding: Non-Standard Encoding
    - 10.6. T1573: Encrypted Channel
    - 10.7. T1105: Ingress Tool Transfer
    - 10.8. T1090: Proxy
    - 10.9. T1095: Non-Application Layer Protocol
    - 10.10. T1071.002: Application Layer Protocol: File Transfer Protocols
11. **Exfiltration:**
    - 11.1. T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage
    - 11.2. T1048: Exfiltration Over Alternative Protocol
    - 11.3. T1041: Exfiltration Over C2 Channel
    - 11.4. T1537: Transfer Data to Cloud Account
12. **Impact:**
    - 12.1. T1486: Data Encrypted for Impact
    - 12.2. T1490: Inhibit System Recovery
    - 12.3. T1531: Account Access Removal
    - 12.4. T1485: Data Destruction
    - 12.5. T1491.001: Defacement: Internal Defacement
    - 12.6. T1529: System Shutdown/Reboot
    - 12.7. T1561.001: Disk Wipe: Disk Content Wipe
    - 12.8. T1489: Service Stop
    - 12.9. T1657: Financial Theft

Для полученных техник APT-группировок проведено сопоставление мер защиты с использованием базы MITRE ATT&CK и оценка наличия соответствующих мер защиты в базовых наборах мер защиты Приказов ФСТЭК России №31 и №239. Результаты анализа представлены в таблице:

реализовано в Приказах ФСТЭК

частично реализовано в Приказах ФСТЭК

не реализовано в Приказах ФСТЭК

Мера защиты в базе MITRE ATT&CK	**Техники**	**Наличие меры в Приказе №239**	**Наличие меры в Приказе №31**
M1018 User Account Management	T1021.001, T1021.004, T1047, T1048, T1053, T1072, T1078, T1110, T1199, T1213, T1484.001, T1485, T1489, T1490, T1505.003, T1537, T1543.003, T1548, T1550.002, T1555.003, T1555.005, T1562.001, T1562.004, T1654, T1657	ИАФ.1, ИАФ.4, УПД.1, УПД.4, УПД.5	ИАФ.1, ИАФ.4, УПД.1, УПД.4, УПД.5
M1026 Privileged Account Management	T1003, T1021.001, T1021.002, T1021.003, T1021.006, T1047, T1053, T1059, T1072, T1078, T1136.001, T1136.002, T1190, T1210, T1548, T1550.002, T1569.002	АУД.9 (только 1-я категория значимости)	АУД.9 (только 1-й класс защищенности)
M1031 Network Intrusion Prevention	T1041, T1046, T1048, T1071.001, T1071.002, T1090, T1095, T1105, T1132.001, T1132.002, T1219, T1566, T1570, T1572, T1573	СОВ.1 (только 1-я и 2-я категории значимости)	СОВ.1 (только 1-й и 2-й классы защищенности)
M1030 Network Segmentation	T1021.001, T1021.003, T1021.006, T1046, T1048, T1072, T1095, T1133, T1136.002, T1190, T1199, T1210, T1482, T1489	ЗИС.4 (только 1-я и 2-я категории значимости)	ЗИС.4 (только 1-й и 2-й классы защищенности)
M1017 User Training	T1003, T1027, T1072, T1078, T1204.002, T1213, T1552.001, T1552.003, T1552.005, T1566, T1657	ИПО.1, ИПО.2, ИПО.4 ИПО.3 (только 1-я и 2-я категории значимости)	ИПО.1, ИПО.2 ИПО.3 (только 1-й и 2-й классы защищенности)

Мера защиты в базе MITRE ATT&CK	Техники	Наличие меры в Приказе №239	Наличие меры в Приказе №31
M1028 Operating System Configuration	T1003, T1021.001, T1053, T1087.001, T1087.002, T1135, T1136.002, T1490, T1543.003, T1548, T1552.003, T1574.006	нет	нет
M1047 Audit	T1021.001, T1027, T1053, T1059, T1213, T1482, T1484.001, T1543.003, T1548, T1552.001, T1560.001, T1562.004, T1566	АУД.10	АУД.10
M1027 Password Policies	T1003, T1021.002, T1072, T1078, T1110, T1552.001, T1555.003, T1555.005	ИАФ.0, ИАФ.4	ИАФ.0, ИАФ.4
M1032 Multi-factor Authentication	T1021.001, T1021.004, T1072, T1078, T1110,T1133, T1136.001, T1136.002, T1199, T1213, T1485	нет	нет
M1038 Execution Prevention	T1036.005, T1047, T1059, T1068, T1106, T1204.002, T129, T1490, T1548, T1562.001, T1574.006	ОПС.1 (только 1-я категория значимости)	ОПС.1 (только 1-й класс защищенности)
M1042 Disable or Remove Feature or Program	T1021.001, T1021.003, T1021.004, T1021.006, T1046, T1059, T1133, T1210, T1219, T1505.003, T1555.004	ОПС.2 (только 1-я и 2-я категории значимости)	ОПС.2 (только 1-й и 2-й классы защищенности)
M1022 Restrict File and Directory Permissions	T1036.005, T1048, T1053, T1070.001, T1489, T1548, T1552.001, T1562.001, T1562.004, T1569.002	УПД.5, ЗИС.13 (только 1-я и 2-я категории значимости)	УПД.5, ЗИС.13 (только 1-й и 2-й классы защищенности)
M1040 Behavior Prevention on Endpoint	T1003, T1027, T1047, T1059, T1106, T1204.002, T1486, T1543.003, T1569.002	АВЗ.3 (только 1-я категория значимости)	АВЗ.3 (только 1-й класс защищенности)
M1051 Update Software	T1068, T1072, T1189, T1190, T1210, T1548, T1550.002, T1555.003, T1555.005	АУД.2, ОПО.0, ОПО.4	АУД.2, ОПО.0, ОПО.4
M1037 Filter Network Traffic	T1021.002, T1048, T1090, T1095, T1219, T1537, T1570, T1572	ЗИС.6, ЗИС.35	ЗИС.6 (необязательный), ЗИС.35 (только 1-й и 2-й классы защищенности)

Мера защиты в базе MITRE ATT&CK	Техники	Наличие меры в Приказе №239	Наличие меры в Приказе №31
M1021 Restrict Web-Based Content	T1059, T1189, T1555.003, T1566, T1567.002	ЗИС.18, ЗИС.23 (необязательный для всех категорий значимости)	ЗИС.18 (необязательный), ЗИС.23 (только 1-й и 2-й классы защищенности)
M1053 Data Backup	T1485, T1486, T1490, T1491.001, T1561.001	ОДТ.4, ОДТ.5	ОДТ.4, ОДТ.5
M1024 Restrict Registry Permissions	T1112, T1489, T1562.001, T1562.004	УПД.5, ЗИС.13 (только 1-я и 2-я категории значимости)	УПД.5, ЗИС.13 (только 1-й и 2-й классы защищенности)
M1041 Encrypt Sensitive Information	T1003.003, T1070.001, T1213	ЗИС.19 ЗНИ.4 (необязателен для всех классов защищенности)	ЗИС.19 ЗНИ.4 (необязателен для всех классов защищенности)
M1048 Application Isolation and Sandboxing	T1021.003, T1068, T1189, T1190	ЗИС7 (необязателен для всех категорий значимости)	ЗИС7 (необязателен для всех категорий значимости)
M1050 Exploit Protection	T1068, T1189, T1190, T1210	СОВ.1 (только 1-я и 2-я категории значимости)	СОВ.1 (только 1-й и 2-й классы защищенности)
M1054 Software Configuration	T1213, T1537, T1555.005, T1566	УКФ.2	УКФ.2
M1057 Data Loss Prevention	T1005, T1041, T1048, T1537	ЗИС.17 (необязателен для всех категорий значимости)	ЗИС.17 (необязателен для всех категорий значимости)
M1035 Limit Access to Resource Over Network	T1021.001, T1021.002, T1133	ИАФ.2	ИАФ.2
M1045 Code Signing	T1036.005, T1059, T1543.003	ОЦЛ.1	ОЦЛ.1
M1015 Active Directory Configuration	T1003, T1072, T1078	нет	нет

Мера защиты в базе MITRE ATT&CK	Техники	Наличие меры в Приказе №239	Наличие меры в Приказе №31
M1049 Antivirus/ Antimalware	T1027, T1059, T1566	АВЗ.1, АВЗ.2, АВЗ.4	АВЗ.1, АВЗ.2, АВЗ.4
M1016 Vulnerability Scanning	T1190, T1210	АУД.2	АУД.2
M1019 Threat Intelligence Program	T1068, T1210	нет	нет
M1020 SSL/TLS Inspection	T1090, T1573	АУД.5 (только 1-я категория значимости)	АУД.5 (только 1-й класс защищенности)
M1029 Remote Data Storage	T1070.001, T1072	ДНС.3 (только 1-я и 2-я категории значимости) ДНС.5	ДНС.3 (только 1-й и 2-й классы защищенности) ДНС.5
M1033 Limit Software Installation	T1059, T1072	ОПС.2, УКФ.3	ОПС.2, УКФ.3
M1036 Account Use Policies	T1078, T1110	УПД.1, УПД.4, УПД.5	УПД.1, УПД.4, УПД.5
M1052 User Account Control	T1548, T1550.002	УПД.4, УПД.5, УПД.11	УПД.4, УПД.5, УПД.11
M1060 Out-of-Band Communications Channel	T1213, T1489	ДНС.4 (только 1-я и 2-я категории значимости)	ДНС.4 (только 1-й и 2-й классы защищенности)
M1013 Application Developer Guidance	T1078	да[15]	нет
M1025 Privileged Process Integrity	T1003.001	ОЦЛ.1 ЗИС.11, ЗИС.12 (необязательны для всех категорий значимости)	ОЦЛ.1 ЗИС.11, ЗИС.12 (необязательны для всех классов защищенности)
M1043 Credential Access Protection	T1003.001	ИАФ.4	ИАФ.4

[15] Данная мера защиты реализуется требованиями Приказа ФСТЭК №239 в п. 29.3.

JET
SECURITY
TEAM

security@jet.su
jetcsirt.su