УНИВЕРСИТЕТ ИТМО

Мониторинг и управление уязвимостями в АСУТП

Лившиц Илья Иосифович, д.т.н., ФБИТ
Соколов Егор Олегович, аспирант, ФБИТ
26.05.2022

План презентации

1. Определение объекта исследования
2. Анализ текущего состояния объекта исследования
3. Исследование существующих технологий и мер защиты
4. Предложения по мониторингу и управлению уязвимостями
5. Выводы

1. Определение объекта исследования (1)

Объектом исследований будем полагать системы АСУТП – автоматизированные системы управления технологическим процессом без определения узкой специализации применения по отраслям.

Данные статистики за последние три года:

1. В 2021 г. на Colonial Pipeline проведена атака с использованием **известных** уязвимостей. Рост уязвимостей АСУТП превысил 40% по сравнению с 2020 г. Для 26% уязвимостей исправлений нет. Чаще всего уязвимости обнаруживаются в продуктах Siemens, Schneider Electric.
2. В 2020 г. количество уязвимостей в АСУТП увеличилось на 10,3% по сравнению с 2019 г., опасных – 53,15% (по шкале CVSS). Наиболее частыми воздействиями был вызов отказа в обслуживании (39%) и **обход механизмов защиты** (37%).
3. В 2019 г. опубликовано исследование о неприменимости CVSS для компонентов АСУТП, поскольку оценки не соответствуют степени опасности. Отмечается, что в случае АСУТП наиважнейшим фактором должна быть **доступность** (что отмечено на примере уязвимости CVE-2015-5374, эксплуатируемой в атаках Industroyer / Crashoverride для вывода из строя реле Siemens).

1. Определение объекта исследования (2)

Краткий анализ статистики позволяет перейти к определению наиболее релевантных **предметов исследований** для объектов АСУТП:

1) рост уязвимостей в компонентах (двузначный рост в процентах);
2) возможности обхода механизмов защиты (двузначная доля в процентах);
3) неприменимость многих известных систем оценок.

В развитие данного вывода можно отметить, что общая культура формирования проблемы обеспечения безопасности компонентов АСУТП пока **недостаточно** учитывает риски.

Вообще «проникновение» практик риск-менеджмента в инженерную культуру нельзя полагать достаточной, поскольку наиболее известные в отрасли стандарты ISO/IEC (ГОСТ Р ИСО/МЭК) серии 61508, 61511, 27001, 27005, 31000, 31010 и пр. **не в полной мере** применяются в РФ в настоящее время.

2. Текущее состояния объекта исследования (1)

Специалисты признают, что в АСУТП **невозможно** использовать такие же подходы, как при обеспечении ИБ в корпоративных сетях, но некоторые рекомендации применимы и для объектов АСУТП, в частности:

1) проведение **аудита** (что является обязательным требованием стандартов);
2) **тестирования** проектных решений на стенде (цифровом двойнике);
3) проведение периодических **киберучений**.

Применительно к проблеме обеспечения соответствия (включающей и аудит, и тестирование и иные способы оценивания) весьма важным является вопрос **применимости** встроенных механизмов функциональной безопасности, реализованных противоаварийной автоматической защитой (ПАЗ).

ФСТЭК неоднократно утверждал, что наличие ПАЗ **не является** основанием для вывода о невозможности ущерба при компьютерном инциденте и **не учитывается** как мера защиты. Позиция ФСТЭК о «недоверии» к компенсирующим (дублирующим) мерам предотвращения компьютерных инцидентов, не подверженных компьютерным атакам (ПАЗ, предохранительные клапана и пр.), **не имеет обоснования**.

2. Текущее состояния объекта исследования (2)

В качестве примера рассмотрим известный инцидент: вирус Triton, который был ориентирован на конкретный тип ПАЗ. С учетом того, что ПАЗ поддерживает удаленное конфигурирование, именно на этот «**транспорт**» была направлена атака.

Более того, сетевой протокол «транспорта» **не предусматривал** меры безопасности, хотя эти меры кибербезопасности были описаны еще в 2013 г. и аппаратный ключ контроллера ПАЗ находился в положении, **позволявшем** удаленно осуществлять конфигурирование.
Этот пример подтверждает ранее показанный пример статистики, что около 37% уязвимостей реализуют **вектор обхода механизмов защиты**.

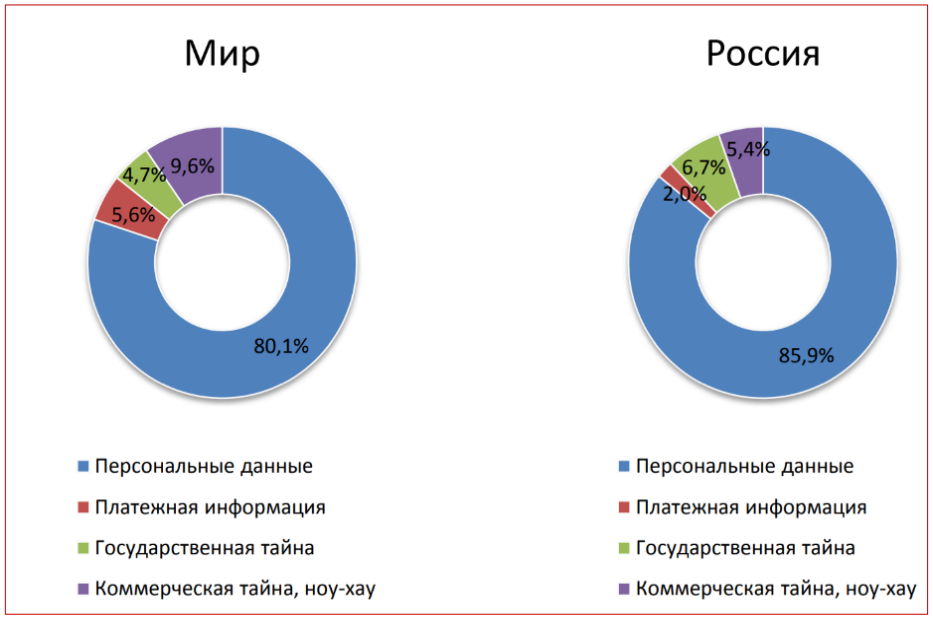
Таким образом, снова можно поднять вопрос о том, какая информация публично доступна в мире и в РФ из потенциально опасной сети интернет.

2. Текущее состояния объекта исследования (3)

В РФ наблюдается ситуация, при которой доля публично доступной в сети интернет **государственной тайны** (6,7%) превышает долю доступной **коммерческой тайны** (5,4%).

Пример – данные InfoWatch за 2021 г.

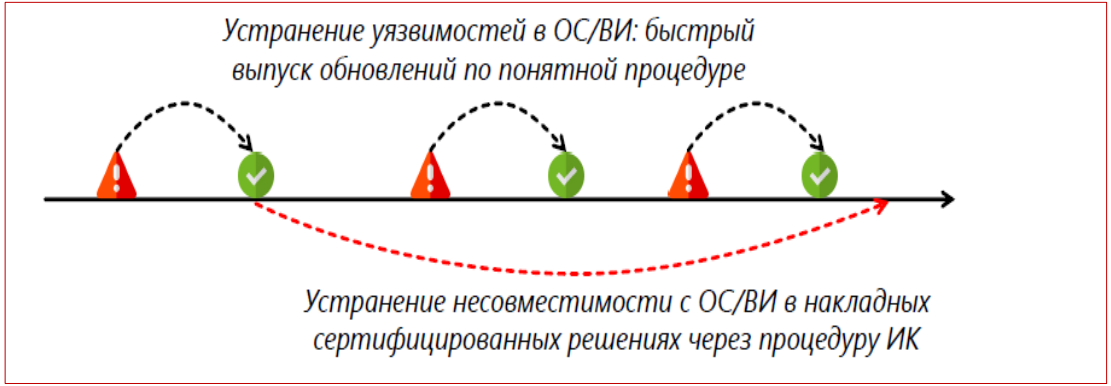
Данный факт отражает как несовершенство применяемых мер защиты, так и **проблемы** выявления и устранения уязвимостей в **ведомственных** информационных системах.



3. Существующие технологии и меры защиты (1)

Рассмотрим идеологию в области технологий и меры защиты, которую сегодня предлагают ведущие мировые и российские поставщики.
Например, в докладе «Актуальные вопросы повышения качества проектов и продуктов по ИБ» («Конфидент») повторяется подход ФСТЭК о «**накладных**» мерах защиты, вводится еще **одна проблема** – устранение уязвимостей в сертифицированных решениях.

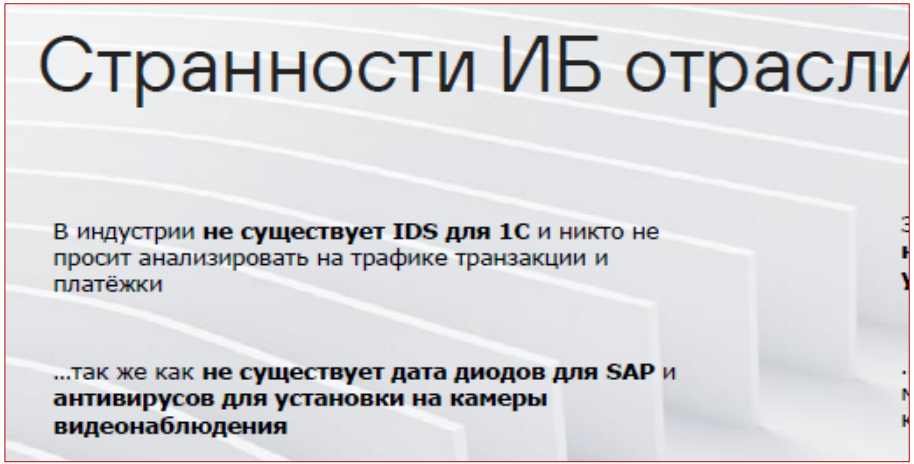
К сожалению, не приводятся никакие оценки **как именно** дополнительные «накладные» меры защиты будут проходить **сертификацию** для конкретных условий функционирования компонентов АСУТП и изменение показателей обеспечения **безопасности** АСУТП в целом.



3. Существующие технологии и меры защиты (2)

В докладе «От защиты АСУ ТП к безопасности предприятия» (Positive) приводится верный тезис: «**в индустрии не существует IDS для 1С и никто не просит анализировать на трафике транзакции и платёжки**».

На практике вся совокупность финансовых транзакций (если верить сообщениям операторов «Диадок», «Тензор» и «Астрал» - это миллиарды документов в год) аккуратно контролируются компонентами ПО в точном соответствии с приказами ФНС, правил ПБУ и пр.



3. Существующие технологии и меры защиты (3)

Очевидно, что «разбирать» каждый план счетов и каждую транзакцию для каждой организации просто **бессмысленно**.

В этой связи разумно задать вопрос – почему же АСУТП попадает в сферу **бесконтрольного** коммерческого интереса поставщиков «накладных» мер защиты, дающих якобы ««универсальный» эффект для всех типов информационных систем?

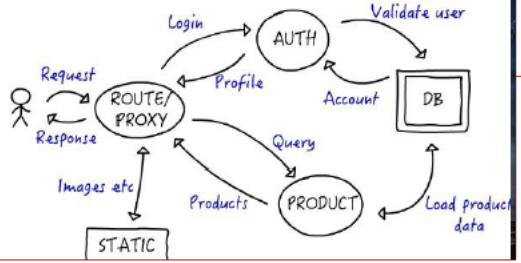
SDLC. Моделирование угроз

Training | Require-ments | Design | Implemen-tation | Verificat

Методологии:

1. STRIDE
2. DREAD
3. PASTA
4. Kill Chain
5. OWASP
6. ..... mixed?

Data Flow Diagram



Первый индустриальный CERT в коммерческой организации

40 экспертов по всему миру в области исследования угроз и уязвимостей, расследования инцидентов и анализа защищенности АСУ ТП

Статус CVE Numbering Authority (CNA)

Обнаружили несколько сотен уязвимостей «нулевого дня» в компонентах АСУ ТП и IIoT

ITMOre than a UNIVERSITY

4. Предложения по мониторингу и управлению уязвимостями (1)

Стандарт IEC 61508-1 определяет все необходимые **термины** для мониторинга и управления уязвимостями:

- **Safety Instrumented System** (SIS) – автоматическая система функциональной безопасности, обеспечивающая применение одной или нескольких автоматических функций безопасности (SIF).
- **Safety Instrumented Function** (SIF) – автоматическая функция безопасности, предназначена для предотвращения наступления или смягчения эффекта для объекта от опасного события посредством его возврата к приемлемому уровню риска.
- **Safety Integrity Level** (SIL) - уровень полноты безопасности, существуют 4 дискретных уровня целостности, связанных с понятием SIL. Чем выше уровень SIL, тем ниже вероятность отказа по запросу (PFD).
- **Probability of Failure on Demand** (PFD) – вероятность отказа при запросе, что система безопасности в случае необходимости не выполнит свою функцию.
- **Average Probability of Failure on Demand** (PFDavg) – средняя вероятность отказа функции при подаче запроса.
- **Safe Failure Fraction** (SFF) – доля неопасных отказов. Рассчитывается из отношения суммы неопасных отказов и диагностированных или распознанных отказов к полной интенсивности отказов системы.

4. Предложения по мониторингу и управлению уязвимостями (2)

Стандарт IEC 61508-1 определяет все необходимые **численные значения** для мониторинга и управления уязвимостями.

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DU} + \lambda_{DD} + \lambda_S},$$

В стандарте IEC 61508-1 определены виды отказов:
— λ_{SU}, безопасные, необнаруживаемые;
— λ_{SD}, безопасные, обнаруживаемые;
— λ_{DD}, опасные, обнаруживаемые;
— λ_{DU}, опасные, необнаруживаемые

Тип A SFF	SIL для симплекса HFT 0	SIL для (m + 1) HFT 1	SIL для (m + 2) HFT 2
<60%	1	2	3
60–90%	2	3	4
90–99%	3	4	4
>99%	3	4	4
Тип B SFF	**SIL для симплекса HFT 0**	**SIL для (m + 1) HFT 1**	**SIL для (m + 2) HFT 2**
<60%	HET*	1	2
60–90%	1	2	3
90–99%	2	3	4
>99%	3	4	4

4. Предложения по мониторингу и управлению уязвимостями (3)

Стандарт IEC 61508-1 явно различает два типа **компонентов**:

1. тип A — характеристика отказа определена полностью и отказы установлены;
2. тип B — компоненты с **неопределенной характеристикой** отказа по крайней мере одного элемента, например, для микропроцессоров.

Учет типа компонента позволяет точно определить соответствующий SIL для компонента АСУТП.
Логично предположить, что этот же подход должен быть применён при оценивании всех компонентов АСУТП, в том числе рекомендуемых «наложенных» средств.
С учётом того, что производители **не приводят реальных данных** по быстродействию и/или надежности своих объектов, уместно предположить, что все они имеют в своём составе как минимум компонент типа B и **должны проходить оценку** по тем же критериям, что и компоненты АСУТП.
Иначе в равнопрочном поле безопасности возникают **неконтролируемые и неоцененные** с точки зрения безопасности области «накладных» мер защиты, в отношении которых не представлены никакие объективные **свидетельства соответствия** установленным требованиям в области безопасности.

4. Предложения по мониторингу и управлению уязвимостями (4)

Национальные стандарты **дают системные требования** по мониторингу и управлению уязвимостями

В ГОСТ РВ 51987–2002 приведена формула:

$$P_{\text{над}} = \frac{T_{\text{нар}}^2}{(T_{\text{вос}} + T_{\text{нар}})(T_{\text{зад}} + T_{\text{нар}})},$$

где:

$T_{\text{нар}}$ — среднее время наработки системы на отказ;

$T_{\text{вос}}$ — среднее время восстановления системы после отказа;

$T_{\text{зад}}$ — задаваемый период надежного функционирования системы.

Соответственно, в идеальном случае $T_{\text{зад}} = T_{\text{нар}}$, а $T_{\text{вос}} \to 0$, тогда $P_{\text{над}} \to 0{,}5$.

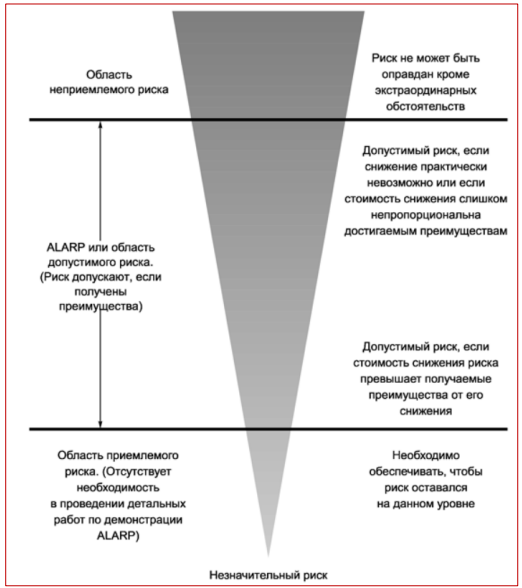
Очевидно, что 50% надёжность – это **нижняя граница любой системы**.

Оценка SIL:

Таблица 3 - Уровни полноты безопасности: целевая мера отказов для функции безопасности, работающей в режиме высокой интенсивности запросов или в режиме с непрерывным запросом

Уровень полноты безопасности	Средняя частота опасных отказов функции безопасности [h^{-1}] (PFH)
4	$>10^{-9}$ - $<10^{-8}$
3	$>10^{-8}$ - $<10^{-7}$
2	$>10^{-7}$ - $<10^{-6}$
1	$>10^{-6}$ - $<10^{-5}$

Оценка рисков:



4. Предложения по мониторингу и управлению уязвимостями (5)

Известны примеры компонентов АСУТП, которые прошли в установленном порядке **оценивание** по требованиям стандарта IEC 61508 и имеют сертификат SIL
Важно обратить внимание, что полученный при **независимой сертификации** уровень SIL дает и поставщику и владельцу объекта КИИ широкий диапазон допустимых вариантов обеспечения безопасности.
Известно, что SIL 4 является самым высоким уровнем снижения риска, который может быть достигнут посредством применения SIS. Но эксперты полагают, что достижение уровня SIL 4 **не всегда** является реалистичным, и в настоящее время существует малое число систем, которые поддерживают этот уровень (как правило, по причине исключительно высокой стоимости).
В тоже время, если «защищаемый» процесс на объекте КИИ несёт в себе такие **высокие риски**, что требуется система уровня SIL 4 для приведения его в безопасное состояние, то в большинстве случаев проблему решают путем **изменения процесса** или применения других (не автоматических) методов снижения рисков. Например, в соответствии с требованиями стандарта IEC (ГОСТ Р МЭК) 31010, определено более 40 методов обработки (снижения) рисков, которые достаточно давно известны и широко представлены в индустрии – например, FMEA, FTA, HAZOP и пр.

5. Выводы

- Прекратить искусственно разделять «вид безопасности» ИТ, ИБ и ФБ. «Латание» уязвимостей «наложенными» мерами (не затрагивая архитектуру, без безопасного проектирования и аудита), не приведет к успеху.
- Применять риск-ориентированные стандарты и экспертизу для компонентов АСУТП, уйти от фиксированных моделей угроз и применения «наложенных» мер с неоцененным уровнем безопасности.
- Предоставить разработчикам компонентов АСУТП возможности независимой оценки соответствия по требованиям признанных стандартов для объективной оценки безопасности объектов КИИ

Спасибо за внимание!

Лившиц Илья Иосифович, д.т.н., ФБИТ

Тел. +7 (921) 934-48-46

ITMOre than a UNIVERSITY