DOI 10.37882/2223–2966.2021.07.37

ПРИМЕНЕНИЕ ДИАГРАММ ЭЙЛЕРА-ВЕННА ПРИ РЕШЕНИИ ЗАДАЧИ ВЫБОРА МЕР ЗАЩИТЫ АСУ ТП[1]

Чернов Денис Владимирович
Соискатель, Тульский Государственный Университет
cherncib@gmail.com

Аннотация. В статье предложено решение задачи выбора мер защиты автоматизированных систем управления технологическими процессами, основанный на построении диаграмм Эйлера-Венна. Предложенное автором решение позволяет увеличить степень защищенности информационных ресурсов АСУ ТП и поднять общий уровень информационной безопасности промышленных систем управления. Проведен обзор наиболее известных фактов успешных атак на АСУ ТП за 1 квартал 2021 года. Цель исследования заключается в исследовании процесса выбора мер защиты на каждом уровне АСУ ТП с применением теории множеств в рамках анализа базовых наборов мер защиты.

Ключевые слова: автоматизированные системы управления, информационная безопасность, технологический процесс, мера защиты, базовый набор, диаграмма Эйлера-Венна.

THE USE OF EULER-VENN DIAGRAMS IN SOLVING THE PROBLEM OF CHOOSING SECURITY MEASURES FOR AUTOMATED PROCESS CONTROL SYSTEMS

D. Chernov

Summary. The article proposes a method for selecting protection measures for automated process control systems based on the construction of Euler-Venn diagrams. The method proposed by the author allows to increase the degree of security of information resources of automated process control systems and to raise the overall level of information security of industrial control systems. The review of the most well-known facts of successful attacks on the automated control system for the 1st quarter of 2021 is carried out. The purpose of the study was to develop a method for selecting security measures at each level of the automated process control system using set theory as part of the analysis of basic sets of security measures.

Keywords: automated control systems, information security, technological process, security measure, basic set, Euler-Venn diagram.

Введение

Исполнение требований технической промышленной безопасности, в рамках противостояния техногенным проявлениям негативного характера, авариям или чрезвычайным ситуациям на промышленных объектах, неразрывно связано с обеспечением информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП).

Одним из наиболее важных этапов построения эффективной системы информационной безопасности АСУ ТП является выбор адекватных мер защиты информационных потоков промышленных систем автоматизации, поскольку отсутствие реагирования системы на актуальные угрозы информационной безопасности приводит к серьезным, в том числе и неконтролируемым последствиям для работоспособности АСУ ТП.

В феврале 2021 года неизвестные киберпреступники провели успешную атаку на систему водоносных очистных сооружений в штате Флорида, США. Нарушители системы информационной безопасности осуществили успешную попытку несанкционированного доступа к программному обеспечению для удаленного контроля за процессами очистки воды и повысили уровень содержания гидроксида натрия более чем в 100 раз. Действия злоумышленника могли бы иметь катастрофические последствия, если бы не были во-

[1] Исследование выполнено при финансовой поддержке Минобрнауки России (Грант ИБ) в рамках научного проекта № 15/2020.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+

Рис. 1. Базовые наборы мер для классов защищенности АСУ ТП

время обнаружены оператором водоочистной станции [1]. Согласно результатам проведенного расследования причин и обстоятельств возникновения атаки, злоумышленники получили доступ к SCADA-системам посредством приложения, которым пользовались системные администраторы для удаленного устранения неисправностей в АСУ ТП. Вектор атаки был успешно реализован ввиду того, что в нарушение всех регламентов и требований по информационной безопасности, для удаленного доступа ко всем компьютерам использовался один и тот же пароль, все автоматизированные рабочие места системы имели выход в сети связи международного обмена при отсутствии систем межсетевого экранирования АСУ ТП [2]. Президент Microsoft Брэд Смит назвал данный инцидент информационной безопасности «самой крупной и изощренной атакой, которую когда-либо видел мир», указывая на то, что подготовку к данной атаке производило более тысячи высококвалифицированных хакеров [3].

Анализируя данную атаку на АСУ ТП, можно сделать вывод об актуальности задачи проведения мероприятий по выбору мер защиты информационной инфраструктуры систем промышленности, в целях минимизации рисков и последствий реализации угроз информационной безопасности АСУ ТП.

Постановка и решение задачи выбора мер защиты

Пусть A — конечное множество мер защиты информации, изложенных в документе [4] $A = \{ИАФ.0; ИАФ.1; .....; ИПО.4\}$ в соответствии с рисунком 1.

Исходя из разделения мер защиты на базовые наборы на основании принятого класса защищенности АСУ ТП, базовые наборы в виде подмножеств множества A представим как:

B — конечное подмножество, включающее в свой состав базовый набор мер, предписанный классу защищенности К3 ($B \subset A$);

C — конечное подмножество, включающее в свой состав базовый набор мер, предписанный классу защищенности К2 ($C \subset A$);

E — конечное подмножество, включающее в свой состав базовый набор мер, предписанный классу защищенности К1 ($E \subset A$).

Рассмотрим задачу, при которой каждый из трех уровней АСУ ТП [5] соответствует разным классам защищенности, а отдельная мера защиты $x \in A$ может быть как характерна для каждого из базовых наборов

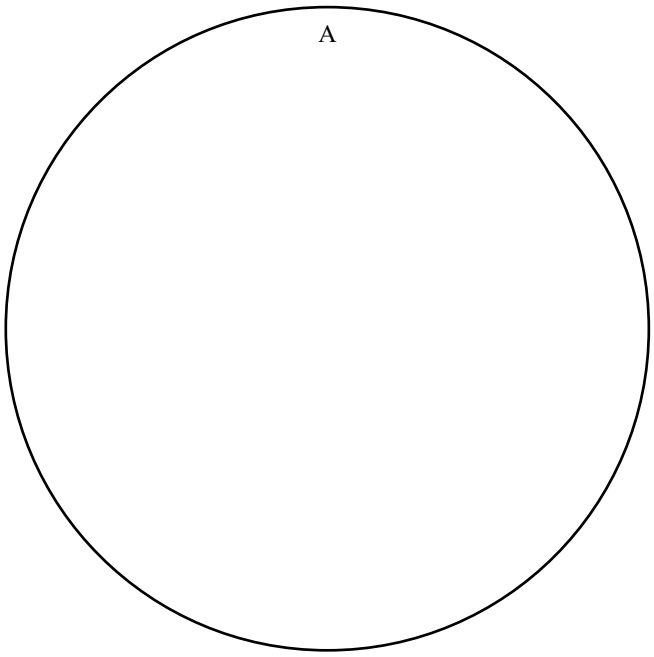

Рис. 2. Диаграмма минимального набора мер защиты АСУ ТП

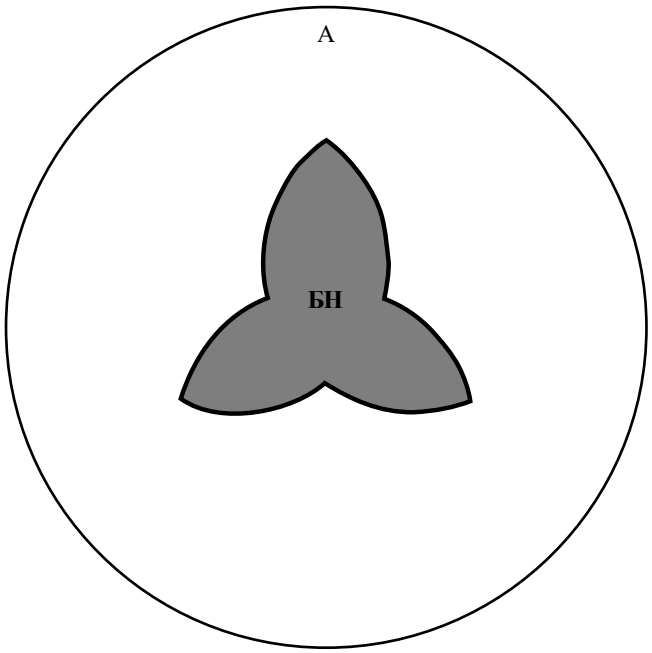

Рис. 3. Диаграмма базового набора мер защиты АСУ ТП

мер защиты, так и быть применима для отдельных базовых наборов тех или иных классов защищенности АСУ ТП. В данной задаче минимальному набору (далее — МН) мер защиты для всех уровней АСУ ТП соответствует следующее пересечение рассматриваемых множеств

$$B \cap C \cap E = \{x \mid x \in B \,\&\, x \in C \,\&\, x \in E\}.$$

Причинами ошибок при определении наборов мер защиты может являться отсутствие наглядного представления пересечений множеств тех или иных мер защиты, присущих каждому из уровней АСУ ТП. Решением данной проблемы является использование диаграмм Эйлера-Венна, которые представляют собой графическое изображение множеств и операций над ними. Идея использования визуального представления множеств принадлежит известному математику Леонарду Эйлеру. Диаграммы или круги Эйлера очень популярны в прикладных науках, в том числе математике, логике и информатике. Диаграммы Эйлера-Венна также используются при представлении связи логических операций с теорией множеств, при доказательстве логических законов и для других важных операций [6,7].

Представим пересечение множеств, соответствующее МН мер защиты в виде диаграммы Эйлера-Венна на рисунке 2.

Как видно из диаграммы МН мер защиты, в данном наборе отсутствуют меры защиты, присущие отдельным уровням АСУ ТП, что приведет к гарантированному наличию уязвимостей в системе. Базовый набор (далее — БН) мер защиты для АСУ ТП, в который включаются все меры, необходимые хотя бы для двух из уровней системы, исключает указанные недостатки МН и представляется в соответствии с выражением

$$(B \cap C) \cup (C \cap E) \cup (B \cap E) = (b \,\&\, e) \cup c) \cup (b \,\&\, e).$$

В целях недопущения дисфункции системы защиты информации введем следующее выражение, описывающее адаптированный базовый набор (далее — АБН) мер защиты АСУ ТП

$$(B \cup C \cup E) \setminus (B \cap C) \cup (C \cap E) \cup (B \cap E).$$

Приведем диаграмму Эйлера-Венна для АБН мер защиты АСУ ТП на рисунке 3.

Исходя из графического отображения АБН, можно сделать вывод о включении в АБН всех мер защиты, имеющих возможность применения на любом из уровней АСУ ТП. Однако, анализируя рисунок 3, можно вывести следующее предположение: АБН не учитывает динамическое изменение условий функционирования АСУ ТП и изменяющие внешние факторы реализации угроз информационной безопасности, что является существенным недостатком реализации системы защиты информации. В целях устранения данного недостатка необходимо проводить этап

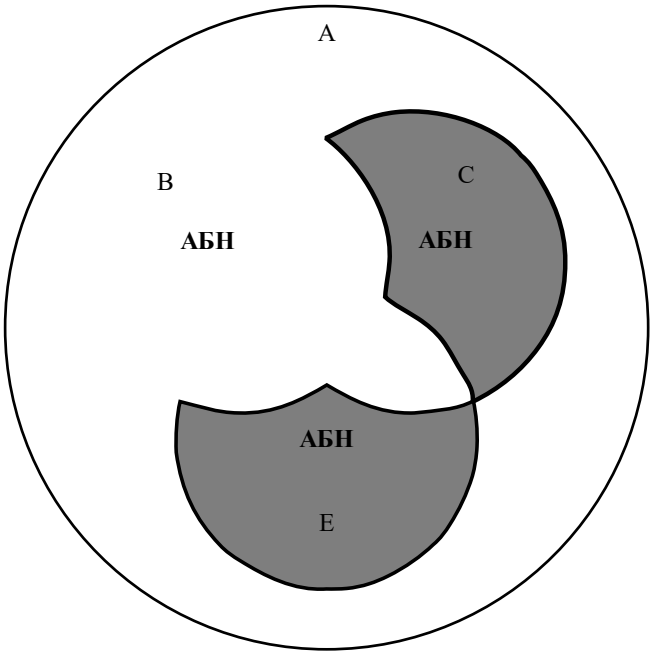

Рис. 4. Диаграмма адаптированного базового набора мер защиты АСУ ТП

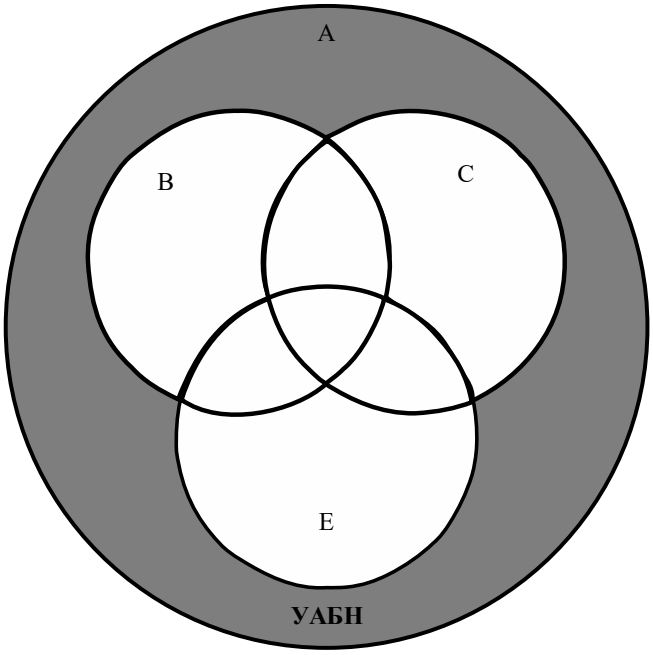

Рис. 5. Диаграмма уточнения адаптированного базового набора мер защиты АСУ ТП

уточнения АБН мер защиты (далее — УАБН) АСУ ТП. УАБН выполняется с учетом результатов оценки возможности АБН нейтрализовать множество угроз характерных для АСУ ТП, или снизить вероятность их реализации, исходя из условий функционирования системы. При УАБН для каждой угрозы из множества, включенной в модель угроз системы, сопоставляется мера защиты из адаптированного базового набора, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации, исходя из условий функционирования АСУ ТП. УАБН осуществляется с учетом не выбранных ранее мер из множества A и определяется следующим выражением. Отображение УАБН мер защиты в виде диаграммы Эйлера-Венна приведено на рисунке 4.

$$A \setminus B \cup C \cup E = \{x \mid x \in A \,\&\, x \notin B \,\&\, x \notin C \,\&\, x \notin E\}.$$

Важно отметить, что обозначение кругов, соответствующих каждому подмножеству из множества мер защиты, возможно в любом порядке.

Заключение

В работе были рассмотрены проблемы обеспечения информационной безопасности автоматизированных систем управления технологическими процессами. Определена актуальность задачи выбора мер защиты промышленных систем, основанная на статистике современных атак на промышленную инфраструктуру. Предложен вариант решения задачи определения мер защиты автоматизированных систем управления технологическими процессами с применением операций математической логики и диаграмм Эйлера-Венна. Результаты исследования рекомендованы для использования при моделировании угроз информационной безопасности и разработке требований к средствам защиты информации в автоматизированных системах управления технологическими процессами.

Acknowledgments: The reported study was funded by Russian Ministry of Science (information security), project number 15/2020.

ЛИТЕРАТУРА

1. Азарова М. Хакеры попытались отравить жителей небольшого города во Флориде // Naked Science — https://naked-science.ru/article/media/hakery-vzlomali-sistemu-vodosnabzheniya — 2021. — 14 мая.
2. Goodin B. Breached water plant employees used the same TeamViewer password and no firewall // Ars Technica — https://arstechnica.com/information-technology/2021/02/breached-water-plant -employees-used-the-same-teamviewer-password-and-no-firewall/ — 2021. — 15 мая.

3. Heath B., Timmons H., Cooney. P. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president // Reuters. Media and Telecoms — https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R — 2021. — 15 мая.
4. Приказ ФСТЭК от 25.12.2014 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // Информационно-правовой портал Гарант.ру — https://base.garant.ru/ 71901880/ — 2021. — 17 мая.
5. Чернов Д.В., Сычугов А.А. Анализ современных требований и проблем обеспечения информационной безопасности автоматизированных систем управления технологическими процессами // Нейрокомпьютеры. Разработка, применение.М.: Радиотехника, 2018. № 8. С. 38–46.
6. Кузьмина Д.В. Использование диаграмм Эйлера-Венна для решения логичеких задач // Вестник современных исследований, 2017. № . 6–1. С. 133–135.
7. Ваулина О.Ю. Решение логических задач на основе диаграмм Эйлера-Венна // Вестник современных исследований, 2017. № . 6–1. С. 113–115.

Журнал «Современная наука: актуальные проблемы теории и практики»

Тульский Государственный университет