

**Содержание**

[Введение 3](#_Toc158767704)

[1 Защита Предприятия путём моделирования атак 5](#_Toc158767705)

[1.1 Цифровая подстанция 5](#_Toc158767706)

[1.1.1 Гипотетическая ситуация 5](#_Toc158767707)

[1.1.2 Устройство цифровой подстанции 5](#_Toc158767708)

[1.2 Цели защиты информационной системы 7](#_Toc158767709)

[1.3 Формирование угроз 8](#_Toc158767710)

[1.3.1 Сценарий атаки «Kill chain» 8](#_Toc158767711)

[1.3.2 MITRE ATT&CK 8](#_Toc158767712)

[1.3.3 Возможные угрозы 9](#_Toc158767713)

[1.3.4 Возможные последствия от атак 11](#_Toc158767714)

[1.3.5 Составление сценария атаки с помощью MITRE Navigator 11](#_Toc158767715)

[1.4 Выводы по разделу 12](#_Toc158767716)

[2 Автоматизация формирования угроз 16](#_Toc158767717)

[2.1 Банк данных угроз информационной безопасности ФСТЭК России 16](#_Toc158767718)

[2.2 Сервисы для помощи в автоматизации формирования сценариев угроз 17](#_Toc158767719)

[2.3 Выводы по разделу 20](#_Toc158767720)

[Список использованной литературы 25](#_Toc158767721)

**Введение**

Учебная практика (ознакомительная практика) относится к разделу Б2.О.01 блока «Практики» базового учебного плана основной профессиональной образовательной программы по направлению подготовки 09.03.03 «Прикладная информатика» и является видом учебной деятельности, направленной на ознакомление, формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью. Учебная практика проходила в Федеральном казенном учреждении «Государственные технологии»

**Цель практики**

Приобретение первичных профессиональных навыков, практического опыта, закрепление, систематизация и расширение теоретических знаний по дисциплинам учебного плана при прохождении учебной практики в Федеральном казенном учреждении «Государственные технологии».

**Задачи практики**

* Закрепление приобретенных теоретических знаний.
* Приобретение навыков научного поиска и практической работы с информационными источниками данных.
* Овладение практическими методиками формирования цели и задач для работы над групповым проектом, управления познавательной деятельностью.
* Приобретение практических навыков участия в командной работе, в групповых проектах, распределения ролей в условиях командного взаимодействия
* Приобретение практических навыков использования иностранного языка при анализе зарубежных информационных Интернет-источников.
* Приобретение навыков использования современных информационных технологий и программных средств для решения задач анализа данных.
* Приобретение навыков инсталлирования программного обеспечения.
* Получение навыков самостоятельной работы.
* Получение навыков подготовки отчетной документации

Источниками информации явились открытые информационные базы, информационно-справочные документы, интернет-ресурсы, учебно-методические материалы, размещенные в Электронном Университете, а также информация, представленная на официальном сайте организации.

**ОСНОВНАЯ ЧАСТЬ**

# Защита Предприятия путём моделирования атак

## Цифровая подстанция

Цифровая подстанция — автоматизированная подстанция, оснащенная взаимодействующими в режиме единого времени цифровыми информационными и управляющими системами и функционирующая без присутствия постоянного дежурного персонала [1].

В нашем случае цифровая подстанция (ЦПС) установлена на электростанции и обеспечивает её бесперебойную и автоматическую работу.

### Гипотетическая ситуация

Для лучшего понимания проблемы определим гипотетическую ситуацию:

В городе Электросталь есть электростанция с ЦПС. Также в этом городе существует организация, предоставляющая услуги облачного центра обработки данных (ЦОД). Услугами данной компании пользуется большое количество других компаний. Злоумышленники могут нарушить работу этих компаний, отключив питание ЦОД путём атаки на подстанцию. Для предотвращения такого негативного воздействия сотрудникам подстанции можно с помощью моделирования сценариев атак разработать соответствующие меры защиты.

### Устройство цифровой подстанции

Вот как выглядит схема работы ЦПС:

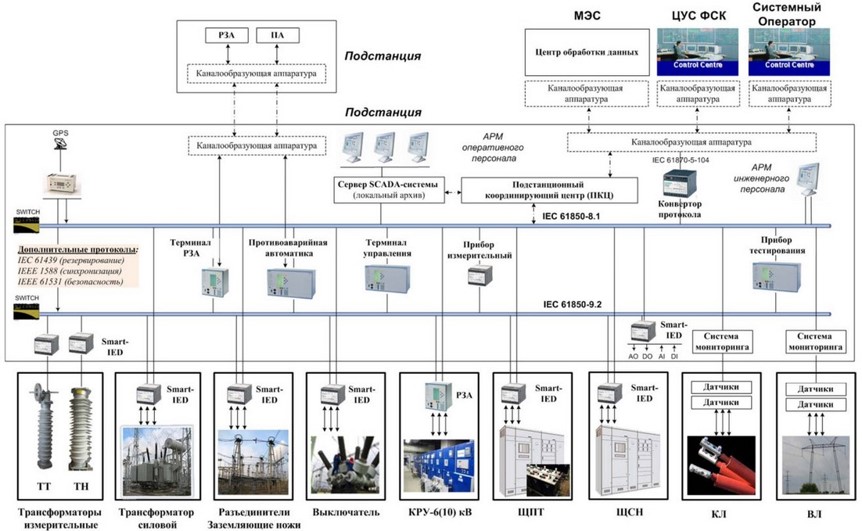


Рис. 1 Схема работы ЦПС [2]



Рис. 2 Обеспечение надёжности и структур [3]

На схеме изображена структура обеспечения надёжности подстанции. Цифровая подстанция на электростанции - сложная, изолированная и самодиагностирующая система с возможностью кратковременного вывода из строя компонентов (вторичного оборудования, то есть, интеллектуальных устройств). (IED - интеллектуальное электронное устройство)

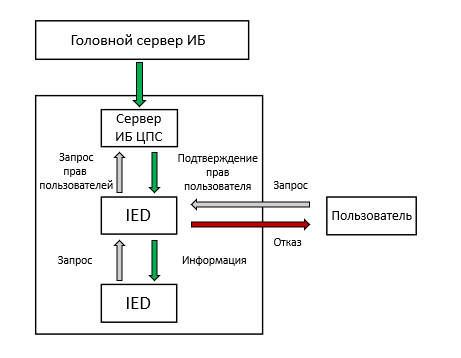


Рис. 3 Схема взаимодействия системы информационной безопасности [3]

Здесь мы можем увидеть схему взаимодействия в системе информационной безопасности подстанции. Главное - то, что у системы есть подтверждение прав пользователей (инженеров с доступом к АРМ, автоматизированному рабочему месту) и возможность отказа в их запросе.

## Цели защиты информационной системы

Прежде чем перейти к основной теме отчёта, необходимо определиться, обязательно ли вообще тратить огромные суммы денег на защиту ИС предприятия. Ведь зная все возможные угрозы на предприятие, менеджерам и руководителям будет проще просто перейти на бумажный документооборот.

На самом деле, нет смысла сразу обеспечивать безопасность от всех угроз. Но определить наиболее слабые места ИС и защитить их обязательно, иначе можно потерять намного больше финансов, чем потратить на защиту от кибератак. Например, в нашей гипотетической ситуации при остановке работы ЦПС, даже на непродолжительное время, пострадают компании, которые получают электричество от электростанции, управляемой ЦПС. К тому же, работа подстанции устроена таким образом, что без обеспечения информационной безопасности (ИБ) её ИС довольно сильно уязвима для атак злоумышленников. Поэтому роль информационной безопасности довольно большая.

## Формирование угроз

### Сценарий атаки «Kill chain»

Злоумышленники пользуются моделью, которую называют “Kill chain” (цепочка убийства), определяющую последовательность действий, ведущих нарушителя к цели. Проще говоря, сценарий атаки. Она состоит из нескольких последовательных этапов:

* Разведка;
* Подготовка к атаке, определение инструментария и доставка;
* Эксплуатация арсенала;
* Установка;
* Управление через командные серверы;
* Горизонтальное перемещение, распространение внутри сети;
* Целевое воздействие.

[4]

### MITRE ATT&CK

В матрице MITRE ATT&CK[5] обозначены похожие этапы.

Вот как выглядит сайт их официальный сайт:

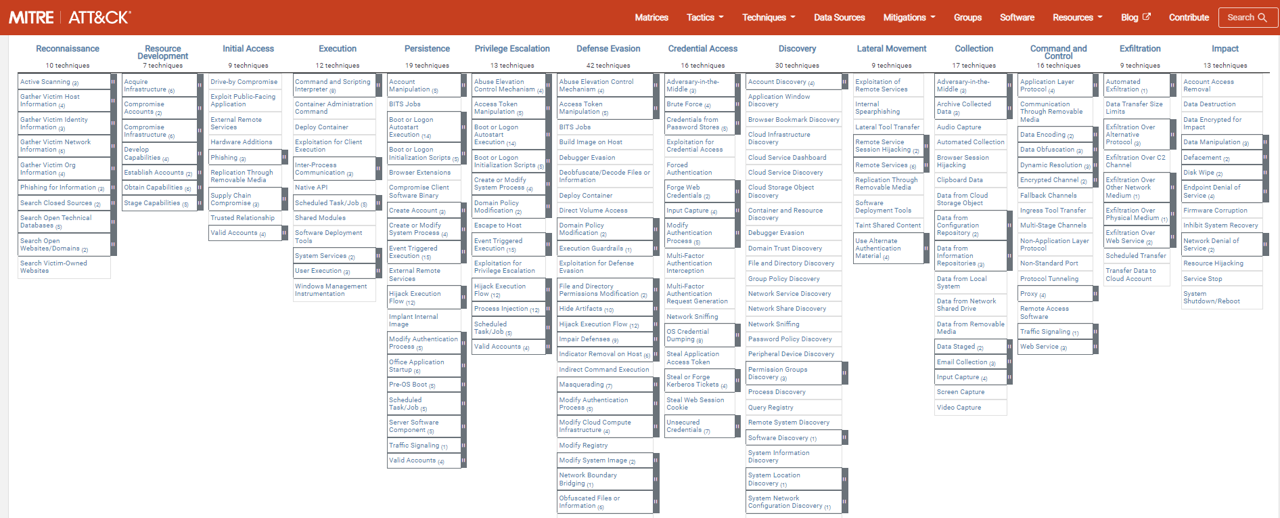


Рис. 4 MITRE ATT&CK

Он представляет собой матрицу с техниками атак. Некоторые техники можно раскрыть и увидеть подтехники. Столбцы представляют собой этапы атак злоумышленников. На скриншоте изображена матрица для предприятий. Всего есть 3 матрицы:

* Enterprise (предприятия);
* Mobile (переносные устройства);
* ICS (индустриальные системы).

Каждая определяет техники, тактики и процедуры для своего случая.

Нас интересует третий вариант.

### Возможные угрозы

Пользуясь информацией о том, что микроконтроллеры подстанции используют самодиагностику, а именно сравнивают полученные сигналы с тестовыми согласно модели, можно подменить модель, и таким образом микроконтроллеры будут отправлять неправильные сигналы компонентам электростанции. Следовательно, работа электростанции остановится. Ещё можно нарушить работу программируемых устройств автоматики. Это тоже вызовет нарушение или остановку работы электростанции.

Также возможна атака воздействием на поставки. На сайте, посвящённом подстанции М. П. Сморгунова, можно увидеть, как много компонентов от разных компаний используется в работе подстанции:

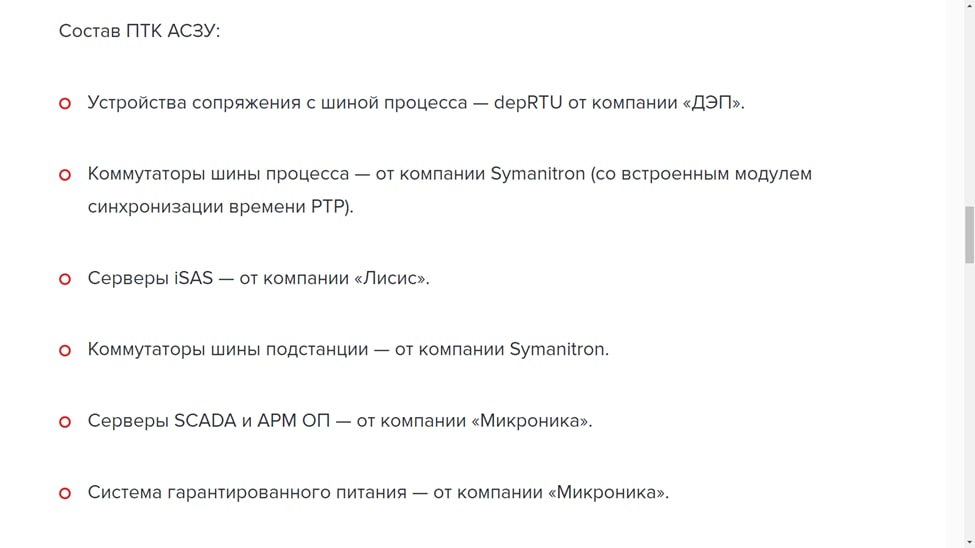


Рис. 5 Поставщики оборудования для подстанции С. М. Сморгунова

Из-за участия сторонних компаний в устройстве ЦПС существуют некоторые риски для самой подстанции. Например, уязвимости программ и компонентов, утечка их работы от бывших сотрудников компаний и т. д.

Возможные техники взлома ЦПС с сайта MITRE ATT&CK, используя MITRE Navigator[7]:

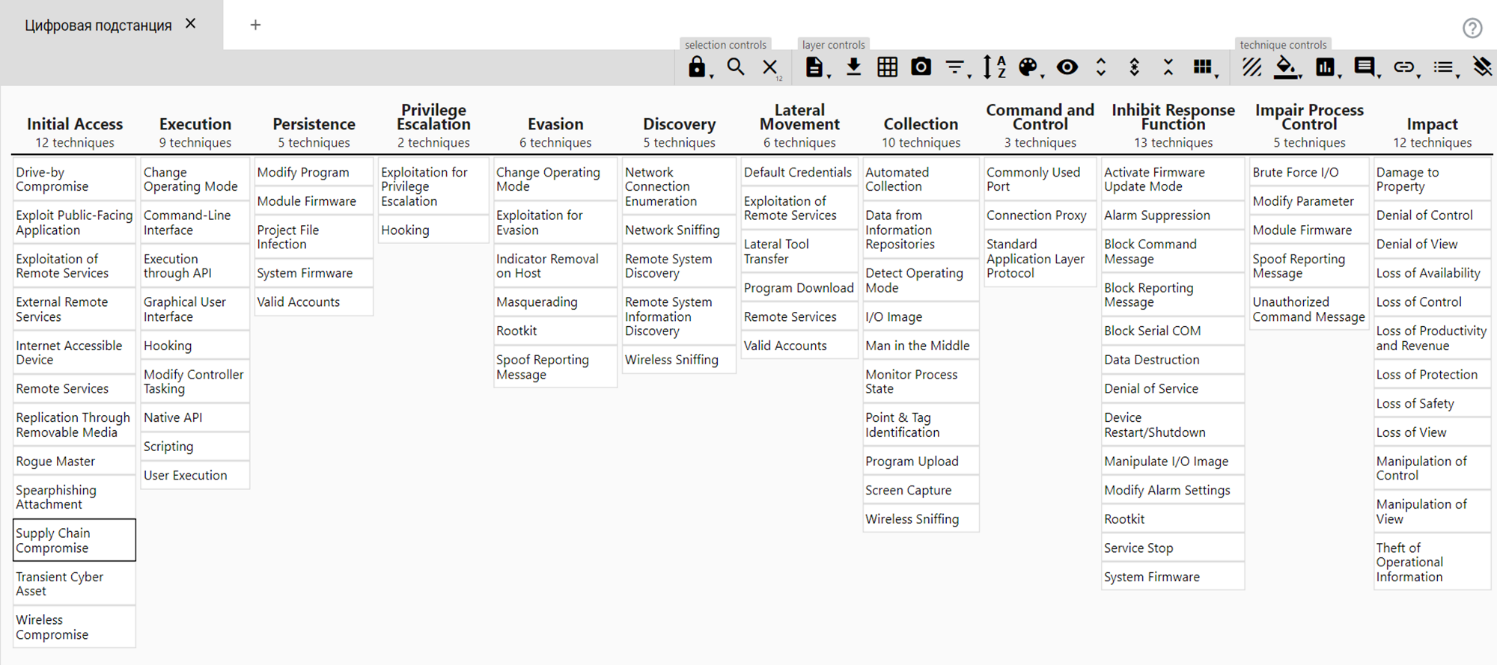


Рис. 6 Матрица MITRE ATT&CK для ICS

Так как системы мониторинга и диагностики оборудования, установленные на цифровой подстанции, являются интеллектуальными, то их тоже можно взломать. Они подключены к датчикам и серверам, а значит, путём неправильной настройки через сервера, можно нарушить их работу.

Одним из возможных сценариев атаки на цифровую подстанцию является использование недекларированных возможностей прикладного ПО (программного обеспечения). По ФСТЕКу[8] СП.6.3; группа способов: использование недекларированных возможностей; способ реализации: использование недекларированных возможностей прикладного программного обеспечения; уровень возможностей нарушителя: B.4 (Нарушитель, обладающий высокими возможностями).

Как вариант, подобное ПО может быть установлено на сервера и посредством использования бэкдора (дыры в программе, незамеченной или намеренно оставленной разработчиком программного обеспечения), злоумышленник может повлиять на работу электростанции.

### Возможные последствия от атак

Возможные последствия от атаки на цифровую подстанцию: выведение из строя оборудования посредством неправильной настройки микроконтроллеров и устройств автоматики, подмены моделей самодиагностики, вызова перегрузки в сети; кражи конфиденциальной информации об электростанции или о ее сотрудниках и передачи третьим лицам; а от вывода из строя работы электростанции - обесточивание инфраструктур, подключенных к ней.

### Составление сценария атаки с помощью MITRE Navigator

С помощью MITRE Navigator[7] был составлен примерный сценарий атаки через изменение модели самодиагностики микроконтроллеров компонентов:



Рис. 7 Сценарий угрозы на MITRE Navigator

Для начала злоумышленники, завладев информацией от бывшего сотрудника электростанции об устройстве сети её ЦПС, пишут вредоносный код и заражают флеш-накопитель инженера, имеющего доступ к серверу цифровой подстанции (например, с помощью фишинга через веб-браузер). Затем сотрудник, при подключении флеш-накопителя, заражает АРМ, а после сам сервер. Предварительно с помощью эксплойтов (дыр в программном обеспечении) вирус повышает свои привилегии, скрывается при помощи руткита (замены интерфейса) и маскировки под другой файл, и заражает микроконтроллеры. Дальше вирус снова скрывается и далее модифицирует модель тестирования для самодиагностики микроконтроллеров. После чего микроконтроллеры передают на компоненты электростанции (например, измерительные трансформаторы, рис. 1) неправильные сигналы, и электростанция прекращает функционирование.

## 1.4 Выводы по разделу

Для того, чтобы обеспечить безопасность информационной системы предприятия, нужно моделировать сценарии атак. Таким образом можно предотвратить нежелательное вмешательство злоумышленников и нарушение работы предприятия. Основываясь на информации в данном разделе, можно сделать следующие выводы (табл.1.1).

Таблица 1.1

Выводы по разделу 1

|  |  |  |
| --- | --- | --- |
| Выводы | Код и наименование компетенции выпускника программы бакалавриата | Код и наименование индикатора достижения компетенции |
| * Определился с целями защиты информационной системы предприятия; * Понял, как обеспечивать защиту информационных систем с помощью моделирования сценариев угроз; * Сформулировал возможные угрозы и их последствия для цифровой подстанции, в том числе с помощью программ; * Составил сценарий атаки на цифровую подстанцию, пользуясь сайтом MITRE Navigator. | ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности; | ОПК-2.1.  Знает принципы работы современные информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности.  ОПК-2.2.  Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.  ОПК-2.3.  Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности. |
| ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | ОПК-3.1.  Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.  ОПК-3.2.  Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.  ОПК-3.3.  Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. |
| УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) | УК-4.1.  Знает принципы построения устного и письменного высказывания на государственном и иностранном языках; требования к деловой устной и письменной коммуникации.  УК-4.2.  Умеет применять на практике устную и письменную деловую коммуникацию.  УК-4.3.  Владеет методикой составления суждения в межличностном деловом общении на государственном и иностранном языках, с применением адекватных языковых форм и средств. |
| Провёл анализ цифровой подстанции, зарубежных и отечественных ресурсов сети интернет. | УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1.  Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.  УК-1.2.  Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности.  УК-1.3.  Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений. |
| * Выполнена постановка задач, сформулирована цель практики * -Распределены функциональные обязанности и сроки составления частей отчёта; сформирован круг задач; заданы временные ограничения; * -Выбраны оптимальные способы решения поставленных задач, исходя из имеющихся возможностей каждого члена команды. | УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.1.  Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.  УК-2.2.  Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.  УК-2.3.  Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах. |
| УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде | УК-3.1.  Знает типологию и факторы формирования команд, способы социального взаимодействия.  УК-3.2.  Умеет действовать в духе сотрудничества; принимать решения с соблюдением этических принципов их реализации; проявлять уважение к мнению и культуре других; определять цели и работать в направлении личностного, образовательного и профессионального роста.  УК-3.3.  Владеет навыками распределения ролей в условиях командного взаимодействия; методами оценки своих действий, планирования и управления временем. |
| УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни | УК-6.1.  Знает основные принципы самовоспитания и самообразования, исходя из требований рынка труда.  УК-6.2.  Умеет демонстрировать умение самоконтроля и рефлексии, позволяющие самостоятельно корректировать обучение по выбранной траектории.  УК-6.3.  Владеет способами управления своей познавательной деятельностью и удовлетворения образовательных интересов и потребностей. |
| УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах | УК-5.1.  Знает основные категории философии, законы исторического развития, основы межкультурной коммуникации.  УК-5.2.  Умеет вести коммуникацию в мире культурного многообразия и  демонстрировать взаимопонимание между обучающимися – представителями различных культур с соблюдением этических и межкультурных норм.  УК-5.3.  Владеет практическими навыками анализа философских и исторических фактов, оценки явлений культуры; способами анализа и пересмотра своих взглядов в случае разногласий и конфликтов в межкультурной коммуникации. |
|
|
| * обоснованы объемы работы по каждой задаче; * Заданы сроки представления результатов своего исследования источников литературы и текста по своей теме; * Заданы временные траектории совместной работы над общим отчётом с учетом требований безопасных условий труда за компьютером и соблюдения режима труда и отдыха для поддержания должного уровня физической подготовленности. | УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни | УК-6.1.  Знает основные принципы самовоспитания и самообразования, исходя из требований рынка труда.  УК-6.2.  Умеет демонстрировать умение самоконтроля и рефлексии, позволяющие самостоятельно корректировать обучение по выбранной траектории.  УК-6.3.  Владеет способами управления своей познавательной деятельностью и удовлетворения образовательных интересов и потребностей. |
| УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности | УК-7.1.  Знает виды физических упражнений; научно-практические основы физической культуры и здорового образа и стиля жизни.  УК-7.2.  Умеет применять на практике разнообразные средства физической культуры, спорта и туризма для сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности; использовать творчески средства и методы физического воспитания для профессионально-личностного развития, физического самосовершенствования, формирования здорового образа и стиля жизни.  УК-7.3.  Владеет средствами и методами укрепления индивидуального здоровья, физического самосовершенствования. |
| УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов | УК-8.1.  Знает причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; основы безопасности жизнедеятельности, телефоны служб спасения.  УК-8.2.  Умеет выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности для обучающегося и принимать меры по ее предупреждению в условиях образовательного учреждения; оказывать первую помощь в чрезвычайных ситуациях.  УК-8.3.  Владеет методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками поддержания безопасных условий жизнедеятельности. |
| УК-9. Способен принимать обоснованные экономические решения в различных областях деятельности | УК-9.1 Знает основные документы, регламентирующие экономическую деятельность; источники финансирования профессиональной деятельности; принципы планирования экономической деятельности  УК-92. Умеет обосновывать принятие экономических решений, использовать методы экономического планирования для достижения поставленных целей  УК-9.3 Владеет навыками применения экономических инструментов |
| УК-10. Способен формировать нетерпимое отношение к коррупционном поведению | УК-10.1 Знает действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности; способы профилактики коррупции и формирования нетерпимого отношения к ней  УК-10.2 Умеет планировать, организовывать и проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе  УК-10.3 Владеет навыками взаимодействия в обществе на основе нетерпимого отношения к коррупции |

# Автоматизация формирования угроз

Как можно автоматизировать формирование сценариев угроз?

Создать программу, которая бы автоматически замечала атаки и вносила их в базу данных навряд ли получится. Такая программа не была бы универсальной для каждого предприятия и случая. Но существуют сервисы для помощи сотрудникам в формировании угроз.

## Банк данных угроз информационной безопасности ФСТЭК России

Рассматривая вопрос автоматизации формирования угроз, мы нашли на сайте ФСТЭК России соответствующий раздел. В нём можно, вводя поэтапно объекты воздействия, компоненты и возможных нарушителей, получить перечень угроз для конкретной ситуации. Мы им воспользовались и получили следующий список:

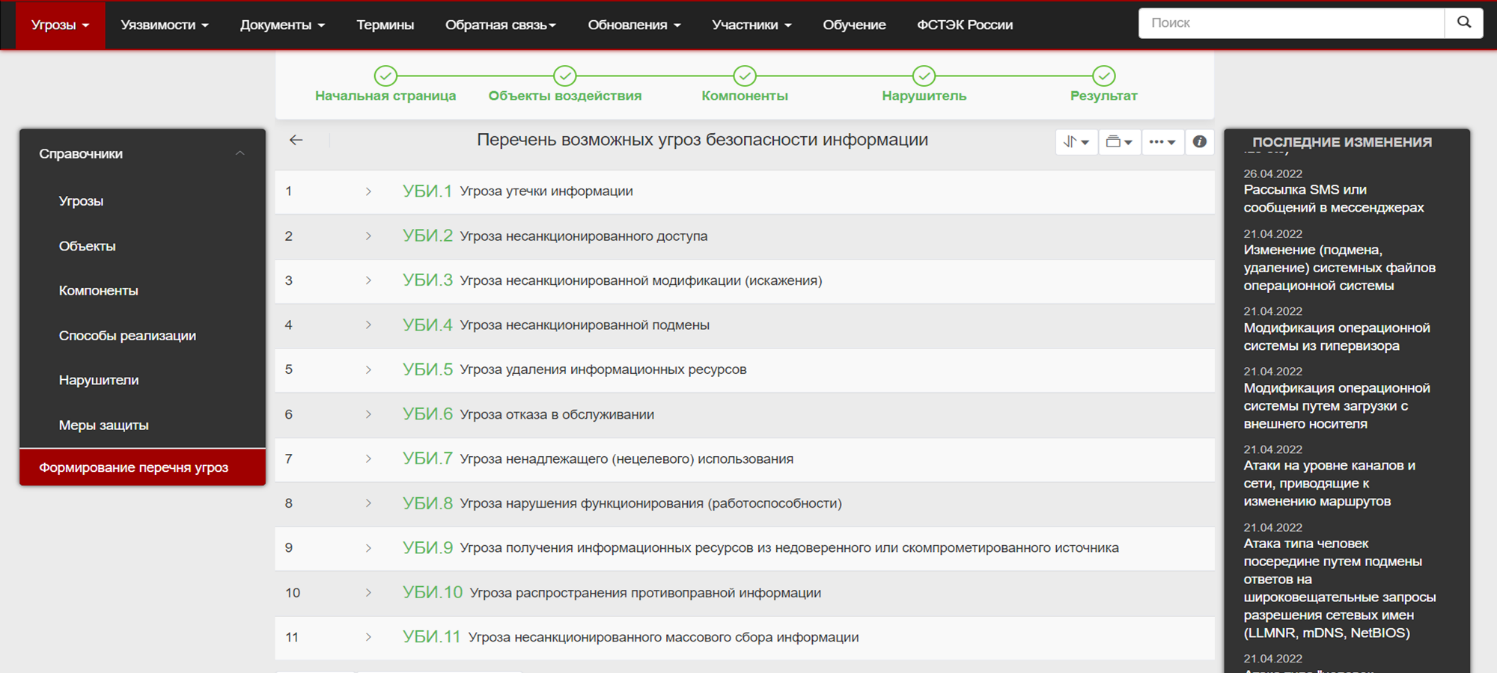


Рис. 8 Перечень возможных угроз для ЦПС от БДУ ФСТЭК [8]

Каждый пункт можно раскрыть, получив конкретные угрозы с описанием, объектами воздействия, компонентами, способами реализации угрозы, уровнями нарушителей и возможными мерами защиты:

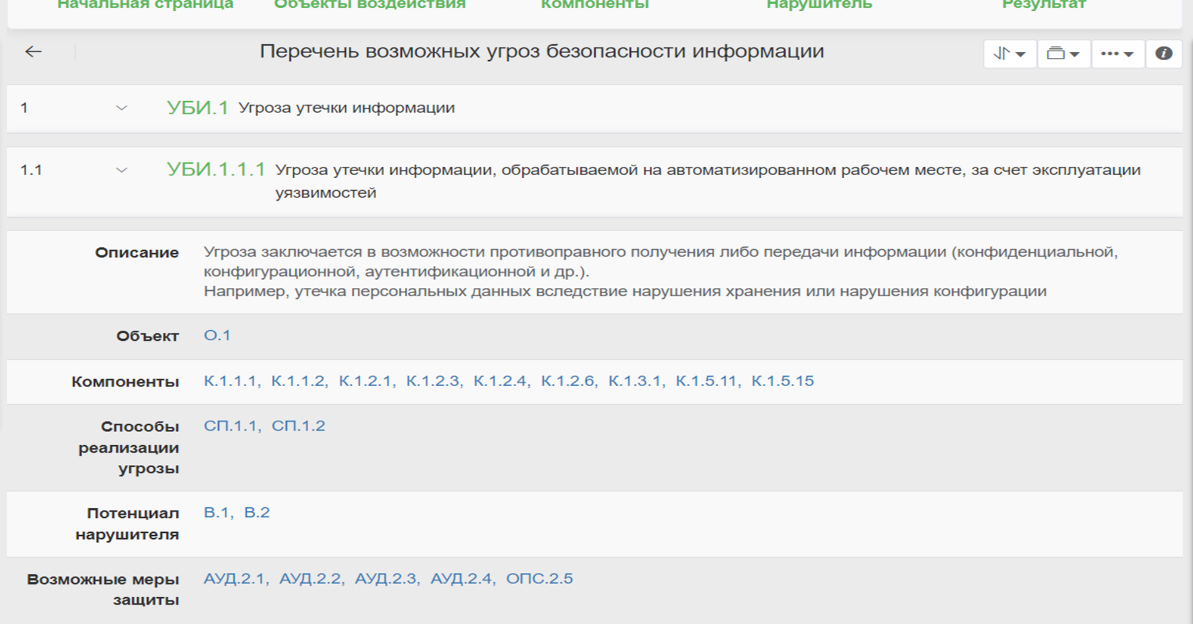


Рис. 9 Пример угрозы от БДУ ФСТЭК (УБИ 1.1.1) [8]

Весь перечень полученных угроз можно скачать в удобном формате, например, в xlsx.

Среди полученных угроз есть даже рассмотренная нами и обозначенная здесь как УБИ.8.1.4 «Угроза нарушения функционирования (работоспособности) автоматизированного рабочего места за счет внедрения вредоносного программного обеспечения». В нашем случае это вредоносный код, который подменит модель тестирования для самодиагностики и приведёт к неправильной работе микроконтроллера(ов) с последующим выводом из строя компонентов электростанции.

## Сервисы для помощи в автоматизации формирования сценариев угроз

На данный момент существует несколько сервисов для ИБ:

* Во-первых, это уже озвученный нами ранее MITRE ATT&CK, который содержит матрицы с техниками атак, и MITRE Navigator, с помощью которого можно наглядно увидеть сценарии атак известных APT-группировок (APT - продвинутая постоянная угроза) и хакерских программ, а также способы борьбы с атаками;
* С помощью показанного нами сервиса ФСТЭК России через удобный интерфейс можно получить перечень возможных атак на предприятие;
* ADTool[9] позволяет построить дерево атак. Программа лёгкая для понимания, имеет понятный интерфейс;

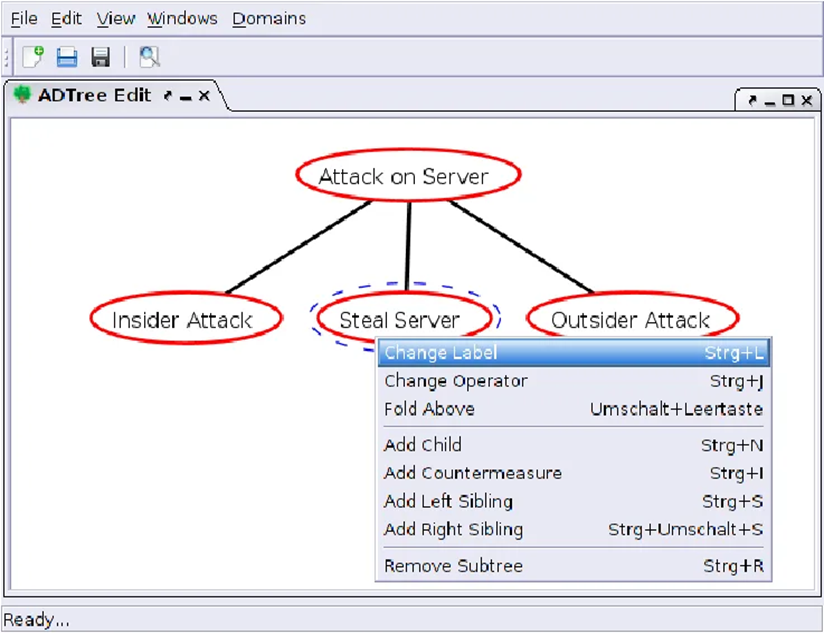


Рис. 10 ADTool

* Правила CAPA[10], проект на GitHub, помогут анализировать исполняемый файл по матрице MITRE ATT&CK;
* MITRE CARET[11] схож с MITRE Navigator и позволяет проследить атаки известных APT-группировок;

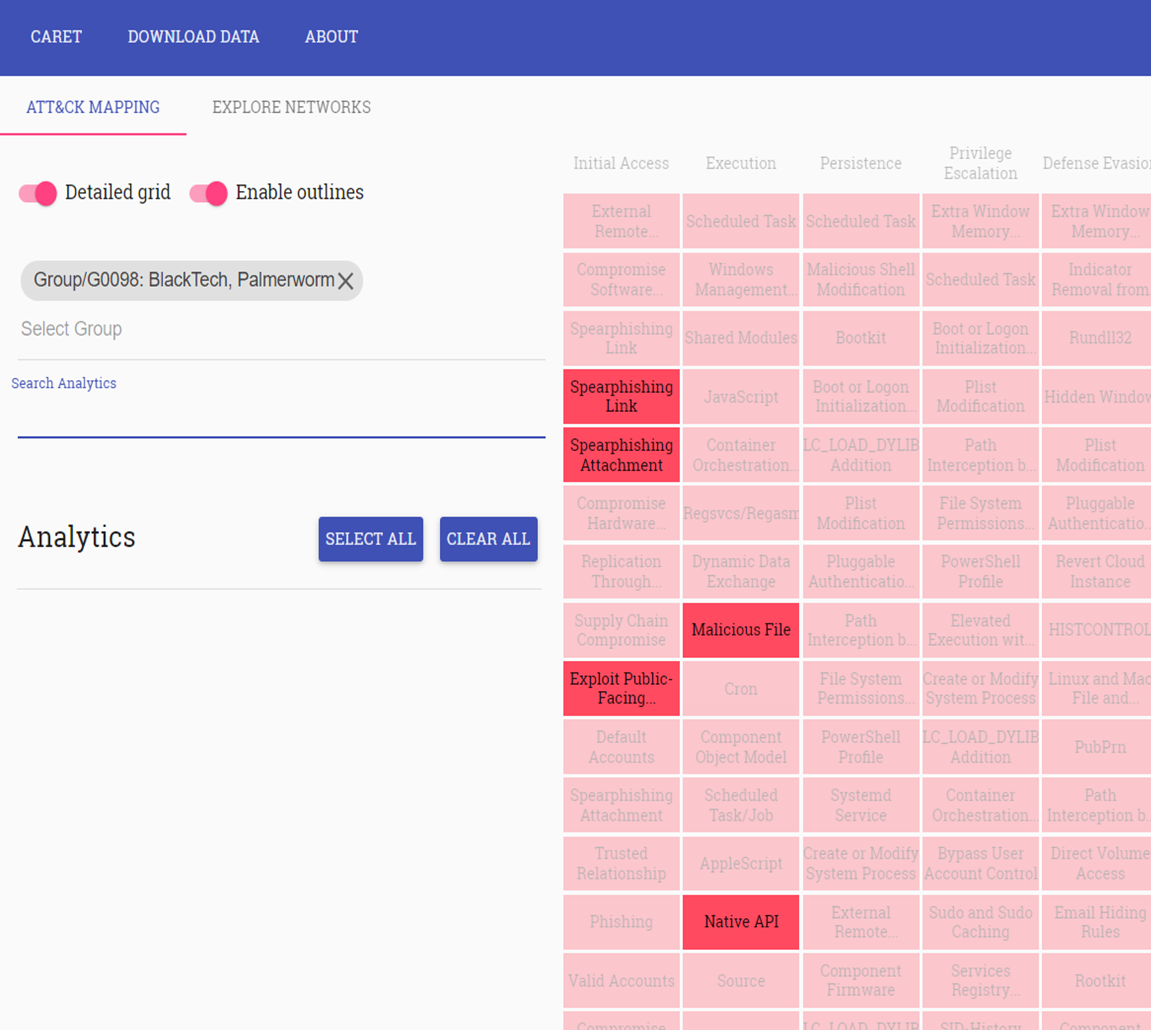


Рис. 11 MITRE Caret

* Microsoft threat modeling tool похож на ADTool, но обладает расширенным функционалом. Программа направлена не на моделирование сценариев угроз, а на поиск уязвимостей. Она помогает находить угрозы при проектировании проектов, предоставляет пользователям возможность обмениваться данными о разработке решений для обеспечения безопасности своих систем и даёт общие рекомендации по анализу проблем, связанных с безопасностью, а также методы их устранения. Среди главных особенностей данного ПО можно выделить:
  + Автоматизацию - рекомендации и отзывы о создании модели;
  + Сдвиг по элементам - интерактивный анализ угроз и их устранение;
  + Отчёты - действия по обеспечению безопасности и тестирование на этапе проверки;
  + Уникальные методы - пользователи могут более эффективно визуализировать и оценивать угрозы.

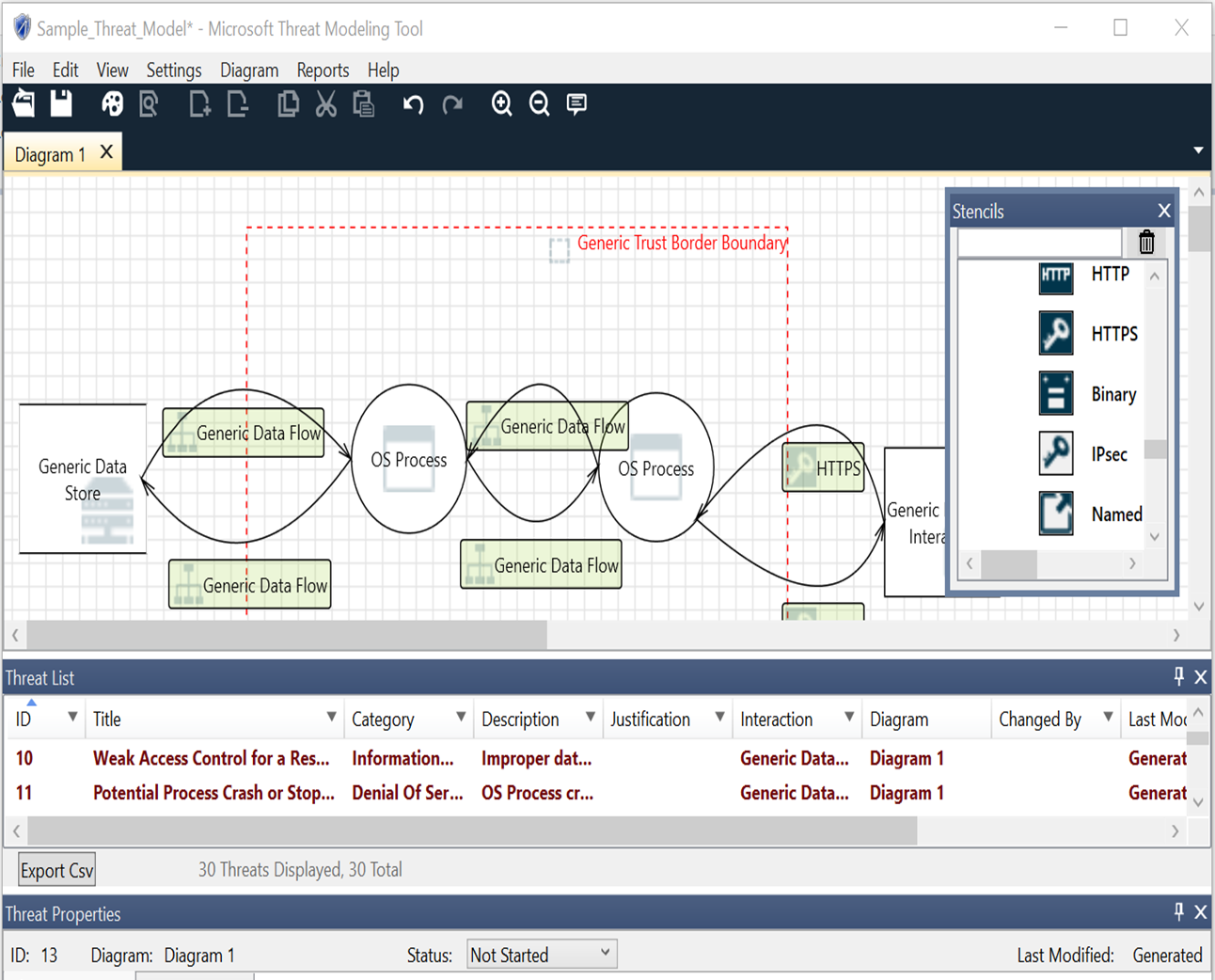


Рис. 12 Microsoft Threat Modeling Tool

## Выводы по разделу

Полностью автоматизировать формирование сценариев угроз и их добавление в базу данных без человека, увы, не получится. Но, пользуясь специальными программами и сайтами, специалисты по информационной безопасности могут упростить этот процесс. Основываясь на информации в данном разделе, можно сделать следующие выводы (табл.2.1):

Таблица 2.1

Выводы по разделу 2

|  |  |  |
| --- | --- | --- |
| Выводы | Код и наименование компетенции выпускника программы бакалавриата | Код и наименование индикатора достижения компетенции |
| * Инсталлировал, изучал и использовал программное обеспечение для моделирования сценариев угроз на примере цифровой подстанции; * Изучал и использовал сайты для моделирования сценариев угроз на примере цифровой подстанции; | ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем; | ОПК-5.1.  Знает основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем  ОПК-5.2.  Умеет выполнять параметрическую настройку информационных и автоматизированных систем.  ОПК-5.3.  Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем. |
| ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности; | ОПК-2.1.  Знает принципы работы современные информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности.  ОПК-2.2.  Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.  ОПК-2.3.  Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности. |
| ОПК-6. Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования; | ОПК-6.1.  Знает основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования.  ОПК-6.2.  Умеет применять методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий.  ОПК-6.3.  Владеет навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий. |
| ОПК-8. Способен принимать участие в управлении проектами создания информационных систем на стадиях жизненного цикла; | ОПК-8.1.  Знает основные технологии создания и внедрения информационных систем, стандарты управления жизненным циклом информационной системы.  ОПК-8.2.  Умеет осуществлять организационное обеспечение выполнения работ на всех стадиях и в процессах жизненного цикла информационной системы.  ОПК-8.3.  Владеет навыками составления плановой и отчетной документации по управлению проектами создания информационных систем на стадиях жизненного цикла. |
| Определив свои задачи, работал с сайтами сети интернет и программным обеспечением для решения поставленных задач, анализа цифровой подстанции и её возможных угроз, последствий, определил меры защиты подстанции. | ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; | ОПК-3.1.  Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.  ОПК-3.2.  Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.  ОПК-3.3.  Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. |
| УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.1.  Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.  УК-2.2.  Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.  УК-2.3.  Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах. |
| Изучал и анализировал сайты сети интернет на русском и английском языках: работал с иностранными MITRE ATT&CK, MITRE Navigator, GitHub, MITRE Caret и отечественным БДУ ФСТЭК России;  Изучал и работал с программой на английском языке: ADTool. | УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) | УК-4.1.  Знает принципы построения устного и письменного высказывания на государственном и иностранном языках; требования к деловой устной и письменной коммуникации.  УК-4.2.  Умеет применять на практике устную и письменную деловую коммуникацию.  УК-4.3.  Владеет методикой составления суждения в межличностном деловом общении на государственном и иностранном языках, с применением адекватных языковых форм и средств. |
| ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью; | ОПК-4.1.  Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.  ОПК-4.2.  Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.  ОПК-4.3.  Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы. |
| УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1.  Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.  УК-1.2.  Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности.  УК-1.3.  Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений. |

**ЗАКЛЮЧЕНИЕ**

**В ходе практики я**:

* Научился закреплять приобретенные теоретические знания.
* Приобрел навыки научного поиска и практической работы с информационными источниками данных.
* Овладел практическими методиками формирования цели и задач для работы над групповым проектом, управления познавательной деятельностью.
* Приобрел практические навыки участия в командной работе, в групповых проектах, распределения ролей в условиях командного взаимодействия
* Приобрел практические навыки использования иностранного языка при анализе зарубежных информационных интернет-источников.
* Узнал об архитектуре цифровой подстанции.
* Научился формировать сценарии атак с помощью программ и сайтов для моделирования сценариев угроз.
* Приобрел навыки использования современных информационных технологий и программных средств для обеспечения информационной безопасности предприятия.
* Приобрел навыки инсталлирования программного обеспечения.
* Научился пользоваться ранее неизвестным мне программным обеспечением.
* Получил навыки самостоятельной работы.
* Получил навыки подготовки отчетной документации.

# Список использованной литературы

1. [СТО 34.01-21-004-2019](https://rosseti.ru/investment/standart/corp_standart/doc/CTO_34.01-21-004-2019.pdf). Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ : стандарт организации ПАО «Россети» : издание официальное : утвержден и введен в действие Приказом ПАО «Россети» от 29.03.2019 № 64: введен впервые : дата введения 2019-03-29 / разработан департаментом оперативно-технологического управления ПАО «Россети» : внесён департаментом оперативно-технологического управления ПАО «Россети». – режим доступа: URL: <https://rosseti.ru/investment/standart/corp_standart/doc/CTO_34.01-21-004-2019.pdf> (дата обращения: 01.06.2022). - Текст : электронный.
2. Цифровая подстанция – важный элемент интеллектуальной энергосистемы / Е. Жукова. – Изображение : электронное // ruscable.ru : [сайт]. - 2017. - 26 сент. - URL: <https://www.ruscable.ru/article/Tsifrovaya_podstantsiya__vazhnyj_element_intellektualynoj_energosiste/#:~:text=Цифровая%20подстанция%20(ЦПС)%20-%20подстанция%2C,каналам%20связи%20на%20единых%20протоколах> (дата обращения: 30.05.2022).
3. Цифровая подстанция – важный элемент интеллектуальной энергосистемы / Ю. И. Моржин. – Изображение : электронное // slideserv.com : [сайт]. – 2014. – 13 августа. – URL: <https://www.slideserve.com/ayoka/3179710> (дата обращения: 30.05.2022).
4. Матрица ATT&CK. Как устроен язык описания угроз и как его используют / О. Борис. – Текст : электронный // xakep.ru : [сайт]. – 2021 – 17 марта. – URL: <https://xakep.ru/2021/03/17/mitre-att-ck/> (дата обращения: 27.05.2022).
5. MITRE ATT&CK : [сайт]. - 2015 - . - URL: <https://attack.mitre.org/> (дата обращения: 27.05.2022). - Текст : электронный.
6. Запущена подстанция имени М. П. Сморгунова / . – Текст : электронный // digitalsubstation.com : [сайт]. – 2017 – 26 декабря. – URL: <http://digitalsubstation.com/blog/2017/12/26/zapushhena-podstantsiya-imeni-m-nbsp-p-nbsp-smorgunova/> (дата обращения 30.05.2022).
7. MITRE Navigator: [сайт]. – 2015 - . – URL: <https://mitre-attack.github.io/attack-navigator/> (дата обращения: 30.05.2022). – Текст: электронный.
8. БДУ ФСТЭК [сайт]. – Москва, 2015 - .- URL: <https://bdu.fstec.ru/threat> (дата обращения: 31.05.2022). Текст: электронный.
9. ADTool 2.2.2 : программа для построения дерева кибер-атак / разработчик The Security and Trust of Software Systems group. - Люксембург : 2017. - Электронная программа : электронная.
10. Capa-rules : [сайт]. – 2020 - .- URL: <https://github.com/mandiant/capa-rules> (дата обращения: 01.06.2022). Текст: электронный.
11. Mitre Caret : [сайт]. – 2015 - .- URL: <https://mitre-attack.github.io/caret/#/> (дата обращения: 01.06.2022). Текст: электронный.
12. Microsoft Threat Modeling Tool: программа, которая помогает находить угрозы на этапе проектирования программных проектов / разработчик Microsoft. – 2016. – Электронная программа: электронная.