МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ДИСПЕТЧЕРИЗАЦИЯ И УПРАВЛЕНИЕ В ЭЛЕКТРОЭНЕРГЕТИКЕ», ПОСВЯЩЕННАЯ 55-ЛЕТИЮ КГЭУ

Казань, 8-10 ноября 2023 г.

Материалы конференции

АО «СО ЕЭС»

НАДЁЖНАЯ СМЕНА

КГЭУ

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский государственный энергетический университет»

МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ДИСПЕТЧЕРИЗАЦИЯ И УПРАВЛЕНИЕ В ЭЛЕКТРОЭНЕРГЕТИКЕ», ПОСВЯЩЕННАЯ 55-ЛЕТИЮ КГЭУ

Казань, 8-10 ноября 2023 г.

Материалы конференции

Казань, 2023

Организаторы конференции

ФГБОУ ВО «Казанский государственный энергетический университет»

АО «Системный оператор Единой энергетической системы»

Благотворительный Фонд «Надежная смена»

При поддержке

Министерство энергетики Российской Федерации

Министерство науки и высшего образования Российской Федерации

Информационный партнер

Журнал «Электроэнергия. Передача и распределение»

УДК 621.3
БКК 31.2
М 43

Рецензенты:
д-р техн. наук, профессор ФГБОУ ВО «КГЭУ» *М. Ш. Гарифуллин*;
канд. техн. наук, доцент ФГБОУ ВО «ИРНИТУ» *В. В. Федчишин*

М 43 **Международная молодежная научно-практическая конференция «Диспетчеризация и управление в электроэнергетике», посвященная 55-летию КГЭУ :** материалы конференции (Казань, 8-10 ноября 2023 г.) / редкол. А. Г. Арзамасова (отв. редактор). – Казань : КГЭУ, 2023. – 726 с.

ISBN 978-5-89873-655-2

Электронное издание

Опубликованы материалы международной молодежной научно-практической конференции «Диспетчеризация и управление в электроэнергетике» по научным направлениям: электроэнергетические системы и сети; генерация, передача и потребление электрической энергии; релейная защита и автоматизация в электроэнергетических системах; электроснабжение и электрооборудование; трансформации в энергетике: экономика, политика, педагогика, коммуникации; первые шаги в электроэнергетику.

Предназначены для научных работников, аспирантов и специалистов, работающих в области энергетики, а также для обучающихся образовательных учреждений энергетического профиля.

Материалы публикуются в авторской редакции. Ответственность за их содержание возлагается на авторов.

УДК 621.3
БКК 31.2

ISBN 978-5-89873-655-2

УДК 621.311.4

ИССЛЕДОВАНИЯ ПО ОЦЕНКЕ ВЛИЯНИЯ КИБЕРАТАК НА ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ, РЕАЛИЗУЕМЫЕ В ПРОЦЕССЕ ДИАГНОСТИКИ ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ

Галяутдинова А.Р.
ФГБОУ ВО «КГЭУ», г. Казань, Россия
Alsu296@yandex.ru,
Науч. рук. проф. Ившин И.В.

В данной работе рассматривается кибербезопасность в системе диагностики энергетического оборудования.

Ключевые слова: диагностика, кибербезопасность, угроза безопасности информации, кибератаки, нарушитель, несанкционированный доступ к информации.

Внедрение различных цифровых решений и технологий в электроэнергетику без использования общих стандартов приводит к проблемам при их интеграции. Важны организационные меры, направленные на координацию цифровой трансформации и создание интегрированной среды, в рамках которой возможно взаимодействие множества различных цифровых сервисов. Обеспечение безопасности цифровых решений является одним из самых больших вызовов нашего времени.

Исследования по оценке влияния кибератак на технологические процессы, реализуемые в процессе диагностики энергетического оборудования, проводятся в форме анализа моделей угроз и нарушителя безопасности информации. Угрозы безопасности информации обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций, а также криминальных группировок, создающими условия для нарушения безопасности информации, которые ведут к ущербу жизненно важным интересам личности, общества и государства[1].

Источниками угроз несанкционированного доступа к информации в объектах информационной инфраструктуры могут быть:

– нарушитель;

– программно-аппаратная закладка;

– носитель вредоносной программы.

Под нарушителем безопасности понимается физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение характеристик безопасности защищаемых информационных

ресурсов. По наличию права постоянного или разового доступа в контролируемую зону источников угроз несанкционированного доступа в информационной системе персональных данных нарушители подразделяются на два типа:

– внешние, которые могут осуществлять атаки из-за пределов контролируемой зоны информационной системы;

– внутренние, которые могут осуществлять атаки, находясь в пределах контролируемой зоны информационной системы.

Различают 4 уровня нарушителей по реализации угроз безопасности информации:

Н1 – обладающий базовыми возможностями, подразумевается наличие возможностей уровня одного человека по приобретению и использованию специальных средств эксплуатации уязвимостей (внешние нарушители, внутренний персонал и пользователи системы, лица, обеспечивающие поставку, сопровождение и ремонт технических средств, бывшие работники);

Н2 – обладающий базовыми повышенными возможностями, подразумевает наличие возможностей реализовывать угрозы, в том числе направленные на неизвестные уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет», но не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей (конкурирующие организации, поставщики вычислительных услуг, услуг связи, лица, обеспечивающие установку, настройку, испытания, пусконаладочные работы, системные администраторы и администраторы безопасности);

Н3 – обладающий средними возможностями, подразумевает наличие возможностей уровня группы лиц по разработке и использованию специальных средств эксплуатации уязвимостей (террористические и экстремистские группы, конкурирующие организации, администраторы системы и разработчики ПО);

Н4 – обладающий высокими возможностями, подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей (работники иностранных технических разведок, спецслужб).

Программно-аппаратная закладка – совокупность технических и программных средств, которые могут осуществлять программно-математические воздействия. Такими возможностями могут обладать разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на источники угроз несанкционированного доступа в информационной системе персональных данных.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Преднамеренное внедрение вредоносных программ в процессе разработки, установки и настройки ПО сводится к минимуму, если все системное и прикладное ПО устанавливается с оригинальных лицензионных дисков, закупленных у официальных дистрибьюторов или надежных поставщиков.

Возможно случайное внедрение программных закладок и вирусов в процессе разработки, установки, настройки, сопровождения и эксплуатации, также велика вероятность внедрения вредоносной программы по сети передаваемыми с файлами, имеющими определенные расширения или иные атрибуты.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям[2]:

$УБИ_i$ = [нарушитель; объекты воздействия; способы реализации угроз; негативные последствия].

Возможными угрозами в отношении электросетевого объекта являются: угрозы несанкционированного доступа к информации на рабочих местах; угрозы, реализуемые в ходе и после загрузки операционной системы и направленные на перехват паролей или идентификаторов; угрозы внедрения вредоносных программ; угрозы выявления паролей и др.[3].

Таким образом, актуальные угрозы безопасности информации представляют собой условия и факторы, создающие реальную опасность несанкционированного доступа к защищаемой информации с целью нарушения конфиденциальности, целостности и доступности. Для нейтрализации актуальных угроз необходимо создание системы защиты информации.

Источники

1. Методический документ «Методика оценки угроз безопасности информации» от 05.02.2021 ФСТЭК России.

2. Банк данных угроз безопасности информации ФСТЭК России [электронный ресурс] http//bdu.fstec.ru (дата обращения: 12.10.23).

Научное издание

МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ
НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«ДИСПЕТЧЕРИЗАЦИЯ И УПРАВЛЕНИЕ
В ЭЛЕКТРОЭНЕРГЕТИКЕ»,
ПОСВЯЩЕННАЯ 55-ЛЕТИЮ КГЭУ

8-10 ноября 2023 г.

Материалы конференции

Публикуются в авторской редакции

Электронное издание

Подписано в печать 28.12.2023.
Формат 60×84/16. Усл. печ. л. 42,2. Уч.-изд. л. 31,58.
Заказ № 501/эл.

Центр публикационной активности КГЭУ
420066, г. Казань, ул. Красносельская, д. 51

ISBN 978-5-89873-655-2