6. О развитии цифровых инноваций в машиностроении в условиях формирования промышленности 4.0 / Б. М. Позднеев [и др.] // Вестн. МГТУ Станкин. – 2019. – №. 2. – С. 23–28.
7. Назаров, И. К. Модель информационной архитектуры процессов взаимодействия на уровне виртуального предприятия / И. К. Назаров, А. О. Коломыцева, М. А. Медведева // Инструменты проектного управления и анализа данных в системах поддержки принятия решений. – 2020. – С. 160–165.
8. Брусакова, И. А. Проблемы внедрения технологических инноваций на цифровом предприятии / И. А. Брусакова // Междунар. конф. по мягким вычислениям и измерениям, 2018 г. / Санкт-Петерб. гос. электротехн. ун-т ЛЭТИ им. В. И. Ульянова (Ленина). – СПб., 2018. – Т. 2. – С. 359–360.
9. Кушнир, К. А.Трансформация промышленных предприятий оборонно-промышленного комплекса Российской Федерации в условиях цифровой экономики / К. А. Кушнир, Е. В. Кобылина // Экономика и менеджмент инновац. технологий. – 2018. – №. 12. – С. 13.
10. Грунтович, Н. В. Экспертные системы управления энергоэффективностью и энергетической безопасностью / Н. В. Грунтович // Энергоэффективность. – 2014. – № 4. – С. 26–30.
11. Optimize the cost of paying for electricity in the water supply system by using accumulating tanks / A. Kapanski [et al.] // In E3S Web of Conferences, 2020 / EDP Sciences. – Les Ulis, 2020. – Vol. 178. – P. 01065.
12. Грачева, Е. И. Анализ и оценка экономии электроэнергии в системах внутризаводского электроснабжения / Е. И. Грачева, А. Н. Горлов, З. М. Шакурова // Изв. высш. учеб. заведений. Проблемы энергетики. – 2020. – № 22 (2). – С. 65–74. https://doi.org/10.30724/1998-9903-2020-22-2-65-74
13. Грачева, Е. И. Применение аналитического метода расчета надежности элементов систем электроснабжения на основе вероятностных моделей / Е. И. Грачева, А. Р. Сафин, Р. Р. Садыков // Надежность и безопасность энергетики. – 2017. – Т. 10, №. 1. – С. 48–52.
14. Fedorov, O. V. Expeditious forecasting of power consumption / O. V. Fedorov // 2017 International Conference on Industrial Engineering, Applications and Manufacturing, May 16–19, Chelyabinsk, Russia, 2017 / IEEE. – Chelyabinsk, 2017. – С. 1–4.

ИНОВАЦИОННЫЕ ТЕХНОЛОГИИ, ОБЕСПЕЧИВАЮЩИЕ КИБЕРБЕЗОПАСНОСТЬ ОБЪЕКТОВ ЭНЕРГЕТИКИ

К. Е. Коршунов

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Т. В. Алфёрова

Представлены основные методы борьбы с кибератаками, выявлены основные проблемы защиты информационной среды промышленных предприятий, определены главные проблемы в кибербезопасности.

Ключевые слова: информационные технологии, кибербезопасность, пентестинг, защита данных, информационная безопасность.

Одними из информационных технологий в области цифровизации электроэнергетики (цифровая энергетика) являются технологии, обеспечивающие кибербезопасность. Цель исследования – привлечение внимания к развитию кибербезопасности в энергетике и возможные методы борьбы с нежелательной утечкой данных.

Кибербезопасность – это реализация мер по защите сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компании. Технологии кибербезопасности являются важнейшим элементом, предоставляющим организациям и отдельным пользователям инструменты, необходимые для защиты от кибератак. Основные компоненты, которые необходимо защитить, – это оконечные устрой-

ства, например, компьютеры, интеллектуальные устройства и маршрутизаторы; сети и облачная среда.

К наиболее распространенным технологиям, используемым для защиты перечисленных компонентов, относятся межсетевые экраны нового поколения, фильтрация DNS, защита от вредоносного ПО, антивирусное ПО и решение для защиты электронной почты. В этом направлении можно выделить несколько основных категорий [1, 4]:

– безопасность сетей – действия по защите компьютерных сетей от различных угроз, например, целевых атак или вредоносных программ;

– безопасность приложений – защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках;

– безопасность информации – обеспечение целостности и приватности данных как во время хранения, так и при передаче;

– операционная безопасность – обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться;

– аварийное восстановление и непрерывность бизнеса – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников;

– повышение осведомленности – обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Доступ злоумышленников к сети промышленного предприятия подразумевает не только утечку данных, но и открытый доступ к микропроцессорной технике, вмешательство в работу которой может иметь серьезные последствия.

Пентестинг включает в себя серию тестов на проникновение, основанных на атаках ИТ-систем для выявления их слабых мест или уязвимостей. Они предназначены для классификации и определения масштабов брешей безопасности, а также их степени влияния. В результате таких тестов предприятие можете получить достаточно четкое представление об опасностях для системы и эффективности вашей защиты [2].

Пентесты помогают определить вероятность успеха атаки, а также выявить дыры безопасности, которые являются следствием уязвимостей с низким уровнем риска, но использующихся определенным образом. Они также позволяют выявлять другие уязвимости, которые невозможно обнаружить с помощью автоматизированного сетевого программного обеспечения или специальных программ, а также могут использоваться для оценки того, способны ли менеджеры по безопасности успешно обнаруживать атаки и эффективно реагировать на них.

Существует несколько типов пентестов, классифицированных в соответствии с типом информации о системе. В whitebox-пентестах известно все о системе, приложениях или архитектуре, а в blackbox-пентестах нет никакой информации о цели. Такой тип классификации – это практическая необходимость, так как условия тестирования основываются на критериях предприятия.

Лаборатория Касперского – международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих киберугроз [3].

Для реализации безопасности предлагается решение, состоящее из двух компонентов:

– KICS for Nodes – компонент защиты конечных узлов технологической локальной вычислительной сетью с загружаемым программным обеспечением;

– KICS for Networks – компонент мониторинга и регистрации событий сетевого обмена с возможностью глубокого анализа прикладных протоколов МЭК 60870-5-104, МЭК 61850 и др.;

– KICS for Nodes – специализированный продукт для промышленных систем. Он представляет собой программное обеспечение, созданное для защиты серверов автоматизированной системы управления технологически процессом, а также операторских панелей и рабочих станций инженеров и операторов под управлением ОС Windows.

Ключевые функции KICS for Nodes:

– белые списки приложений – позволяют запретить запуск всех приложений, помимо явно разрешенных. Этот компонент можно использовать в тестовом режиме, чтобы упростить установку и снизить количество ошибок на этапе внедрения;

– контроль устройств – позволяет администраторам определять, какие устройства разрешено подключать к защищаемым промышленным системам. Технология предотвращает возможность несанкционированного доступа и поддерживает применение масок для удобства управления и оперирования списком устройств;

– контроль беспроводных сетей – позволяет отслеживать любые попытки подключения к неавторизованным сетям Wi-Fi;

– средства обнаружения вредоносных программ – сочетают сигнатурные и эвристические методы защиты и ограждают рабочие станции Windows от известных, неизвестных и сложных угроз. Технология «Анти-Криптор» защищает от попыток атак программ-шифровальщиков;

– межсетевой экран – ограничивает возможность подключиться к узлам промышленной сети;

– проверка целостности ПЛК – обеспечивает дополнительный уровень контроля конфигурации контроллера с помощью периодических проверок изменений в проектах.

KICS for Networks является специализированным программно-аппаратным средством мониторинга сетевого обмена между узлами в промышленной сети систем защиты и управления, которое позволяет определять и регистрировать аномальные и важные с точки зрения обеспечения безопасности эксплуатации оборудования электроустановок и бесперебойного электроснабжения потребителей информационные события. Об обнаруженных отклонениях KICS for Networks оповещает обслуживающий персонал.

Представим список основных функциональных возможностей решения:

1. Мониторинг целостности технологической ЛВС:

– режим самообучения, позволяющий выявить и зарегистрировать все существующие узлы ЛВС и коммуникации между ними, с целью последующего использования этой модели сети в качестве опорной и для отслеживания изменений;

– обнаружение и регистрация подключения новых сетевых устройств к контролируемым сегментам технологической сети;

– обнаружение и регистрация новых сетевых коммуникаций между узлами по признакам: адрес узла-отправителя, адрес узла-получателя, протокол обмена, порт, количество допустимых соединений;

– обнаружение и регистрация сетевых подключений к ИЭУ с использованием прикладных технологических протоколов, используемых для конфигурирования;

2. Анализ прикладных технологических протоколов:

– Разбор, анализ и регистрация важных сообщений прикладных технологических протоколов, в соответствии с конфигурацией и с учетом их возможного влияния на исполнение технологического процесса, а именно:

– обнаружение команд телеуправления оборудованием электроустановки по промышленным сетевым протоколам (МЭК 61850, МЭК 60870-5-104);

– обнаружение команд телеуправления параметрами функционирования системы защиты и управления (например, переключения группы уставок) по промышленным сетевым протоколам (МЭК 61850, МЭК 60870-5-104);

– обнаружение фактов управления и параметрирования ИЭУ сервисным ПО через контролируемый сегмент сети – как при использовании стандартных, так и специализированных протоколов;

– мониторинг сообщений телеизмерений и телесигнализации.

3. Хранение информации о событиях:

– система KICS for Networks обеспечивает хранение выявленных событий во внутренней защищенной базе;

– глубина хранения данных о событиях определяется сроком хранения и верхней границей размера архива;

4. Интеграция с внешними системами и уведомление пользователей:

– KICS for Networks можно интегрировать как один из компонентов в систему управления событиями безопасности (Security information and event management, SIEM) более высокого уровня, – например, HP ArcSight, либо в другую внешнюю систему, поддерживающую стандарт отправки и регистрации сообщений о событиях Syslog;

– уведомление ответственных лиц может быть дополнительно организовано при помощи сообщений электронной почты и SMS.

Таким образом, были выведены основные направления кибербезопасности в энергетике. Кибербезопасность должна стать неотъемлемой частью в защите данных промышленных предприятий. Также для сотрудников, работающих в структурах с использованием облачных хранилищ необходимо проводить краткие тренинги по кибербезопасности с целью исключении человеческого фактора.

Литература

1. Безкоровайный, М. М. Кибербезопасность подходы к определению понятия / М. М. Безкоровайный, А. Л. Татузов // Вопр. кибербезопасности. – 2014. – № 1 (2). – С. 22–27.
2. An overview of penetration testing / A. G. Bacudio [et al.] // International Journal of Network Security & Its Applications. – 2011. – Vol. 3, N 6. – P. 19.
3. Касперский, Е. В. В заложниках у автоматики: как защитить промышленность от кибератак / Е. В. Касперский // Безопасность информ. технологий. – 2016. – Т. 23, № 3. – С. 7–10.
4. Ерохин, П. М. Инновации и инновационные технологии в электроснабжении / П. М. Ерохин, Ю. А. Куликов // Систем. оператор Единой энергосистемы.