# Проектирование и создание подсистемы информационной безопасности для организации защищенного дистанционного управления оборудованием и РЗА и мониторинга устройств МП РЗА на подстанциях 110–220 кВ ПАО «Россети Московский регион»

УДК 621.316.9

**Защита информации и вопросы кибербезопасности сегодня являются определяющими векторами технологического развития в каждой отрасли. Специалисты отмечают ежегодный рост компьютерных атак, направленных на получение личных данных, но и увеличение атак на промышленные объекты и системы с целью захвата управления. Для сферы энергетики в современных условиях особенно остро стоят вопросы надежности и кибербезопасности систем цифрового дистанционного управления энергообъектами. Причиной этому является критичность функций указанных объектов и опасность возможных киберфизических последствий при реализации на них угроз информационной безопасности. В статье рассматривается специфика защиты автоматизированных систем управления на примере организации подсистемы информационной безопасности для защищенного дистанционного управления технологическим оборудованием и системы мониторинга РЗА. Дан краткий обзор современных тенденций в области информационной безопасности АСУ ТП, описаны ключевые особенности построения системы защиты.**

**Гвоздев Д.Б.,**
первый заместитель генерального директора — главный инженер ПАО «Россети Московский регион»

**Широков С.Ю.,**
главный эксперт Управления информационной безопасности и специальных проектов ПАО «Россети Московский регион»

**Грибков М.А.,**
директор Департамента релейной защиты и режимной автоматики электрических сетей ПАО «Россети Московский регион»

**Герасимов О.А.,**
руководитель отдела информационной безопасности ООО «ПиЭлСи Технолоджи»

**Рыбаков А.К.,**
руководитель отдела алгоритмического обеспечения АО «РТСофт»

**Ключевые слова:**
автоматизированные системы, электроэнергетика, дистанционное управление, информационная безопасность (ИБ), РЗА, АСУ ТП

Особенно остро для сферы энергетики в современных условиях стоят вопросы надежности действия и кибербезопасности систем цифрового дистанционного управления энергообъектами. Причиной этому является критичность функций указанных объектов и опасность возможных киберфизических последствий при реализации на них угроз информационной безопасности.

Ведущие игроки рынка информационной безопасности отмечают ежегодный рост компьютерных атак, направленных на промышленные системы. Так, Исследовательский комитет НИК B5 «Релейная защита и автоматика» Международного Совета по большим электрическим системам высокого напряжения определил [1] тематику кибербезопасности как одну из самых актуальных в сфере развития РЗА в мире.

В то же время информация о системах защиты критичных объектов электроэнергетики является конфиденциальной, поэтому в большинстве публикаций не раскрываются детали по защите таких систем, как системы дистанционного управления оборудованием и РЗА. Любая информация о конкретных применяемых средствах и методах защиты может стать для злоумышленников учебным пособием и значимым фактором, повышающим эффективность планируемых атак на объекты критической инфраструктуры. Исполнитель,

реализующий проектирование и внедрение систем защиты дистанционного управления РЗА, как правило, связан обязательствами о неразглашении информации о системе защиты.

С другой стороны, реализация подсистемы (системы) защиты информации является неотъемлемой частью при внедрении дистанционного управления и удаленного мониторинга любого рода информационных ресурсов. Во многих странах мира, в том числе в России, реализация защиты систем дистанционного управления регламентирована на законодательном уровне, а невыполнение установленных требований по защите объектов критической информационной инфраструктуры приводит к штрафам и санкциям. Таким образом изучение требований законодательства к обязательным мерам защиты значимых объектов критической информационной инфраструктуры позволяет сделать обоснованные выводы о составе и функциях применяемых средств защиты, включая средства защиты для объектов, действующих в сфере электроэнергетики. Всесторонний анализ законодательства и находящейся в открытом доступе информации о существующих средствах защиты информации дает возможность сделать выводы в том числе о том, каким образом реализуется безопасность систем дистанционного управления оборудованием и цифровыми устройствами РЗА.

Стоит отметить, что долгое время АСУ ТП считались недоступными для хакерских атак. Миф о защищенности изолированных промышленных систем рухнул в 2010 году в момент выхода их строя центрифуг по обогащению урана на заводе в Иране: инцидент был вызван воздействием компьютерного червя, принесенным на USB-flash-накопителе сотрудником компании-подрядчика.

Другим примером уязвимости промышленного оборудования перед угрозами информационной безопасности может стать авария на подстанции «Пивнична» в Киеве, повлекшая за собой отключение электричества в нескольких районах города и прилегающих областях: ночью с 17 на 18 декабря 2016 года вредоносным ПО были «обнулены» файлы с конфигурациями автоматики и оборудования, отвечающими за подачу электричества.

С тех пор прошло немало времени, но аргумент о необходимости воздушного зазора и изолированности систем АСУ ТП все еще ставится на важное место в вопросах построения промышленных систем и реализации их системы информационной безопасности. Однако с учетом современных тенденций данный подход показал себя не с лучшей стороны.

Основной проблемой «информационной защиты путем информационной изоляции» является ложное чувство безопасности и, как следствие, отсутствие мероприятий по аудиту и оценке уровня защищенности. Развитие технологий приводит к тому, что системы управления окончательно перестают быть изолированными. Так, применение технологий искусственного интеллекта (в частности, нейронных сетей) для анализа данных с датчиков и камер видеонаблюдения требует большого объема данных, которые могут поступать только с нижнего уровня автоматизированных систем.

Совокупность этих факторов ведет к тому, что необходимость защиты промышленных систем больше не может игнорироваться. Как следствие, одним из основных направлений развития современного рынка кибербезопасности становится защита промышленных систем. Данная тенденция поддерживается со стороны ведущих производителей средств защиты информации, производителей средств автоматизации и экспертного сообщества. Особое внимание при этом уделяется корреляции между непосредственно средствами защиты информации и работами, связанными с активным развитием требований к защите информации, предъявляемых к промышленным системам и, в особенности, к электроэнергетике, цифровым подстанциям и их компонентам.

Отдельно стоит отметить, что прошедший 2020 год не стал исключением для угроз кибербезопасности в АСУ ТП. Так, согласно последним данным от Лаборатории Касперского [2], процент используемых для проектирования и интеграции АСУ ТП компьютеров, на которых было заблокировано вредоносное ПО, вырос до 39,3%. На рисунке 1 можно рассмотреть процент компьютеров АСУ, на которых были заблокированы вредоносные объекты.

За последние полгода значительно увеличилось число атак на АСУ ТП в сфере энергетики в сравнении с первой половиной 2020 года.

Активная цифровизация электроэнергетики ведет к ежегодному росту количества объектов, на которых появляются современные системы телеуправления и мониторинга оборудования, призванные предотвратить аварии и последствия от них: человеческие жертвы, повреждение имущества, недоотпуск электроэнергии. В силу особенностей архитектуры и функционала такие системы нуждаются в особом контроле, что подтверждается как на практике, так и в рамках исследований специалистов [3, 4].

Вопросами, связанными с защитой промышленных систем, интересуются не только поставщики

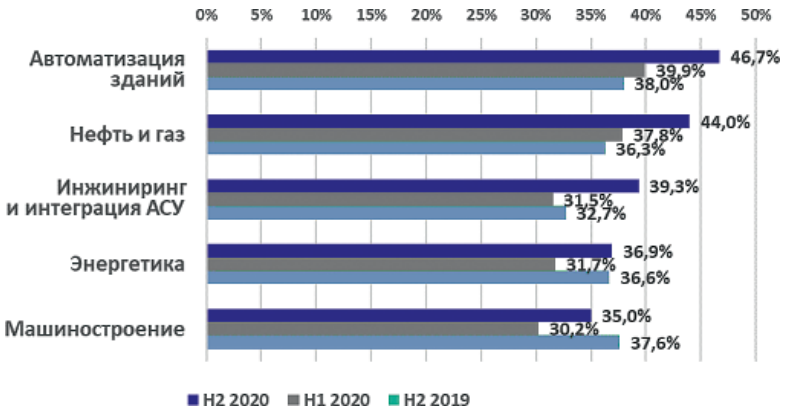


*Рис. 1. Статистика заблокированного вредоносного ПО на АСУ ТП*

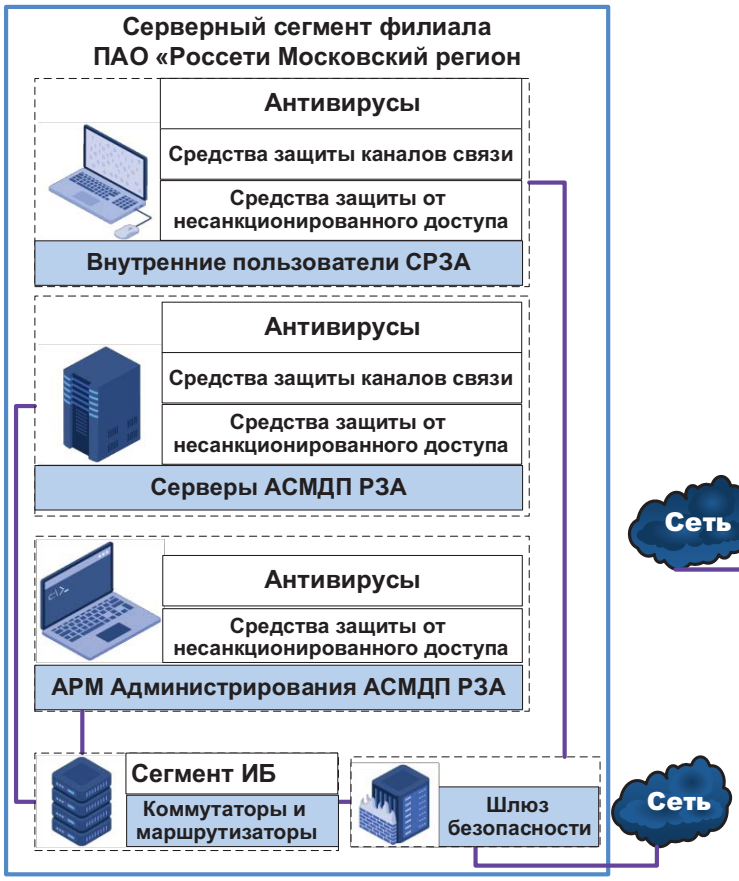


*Рис. 2. Схема защиты серверного сегмента филиала Московские высоковольтные сети ПАО «Россети Московский регион»*

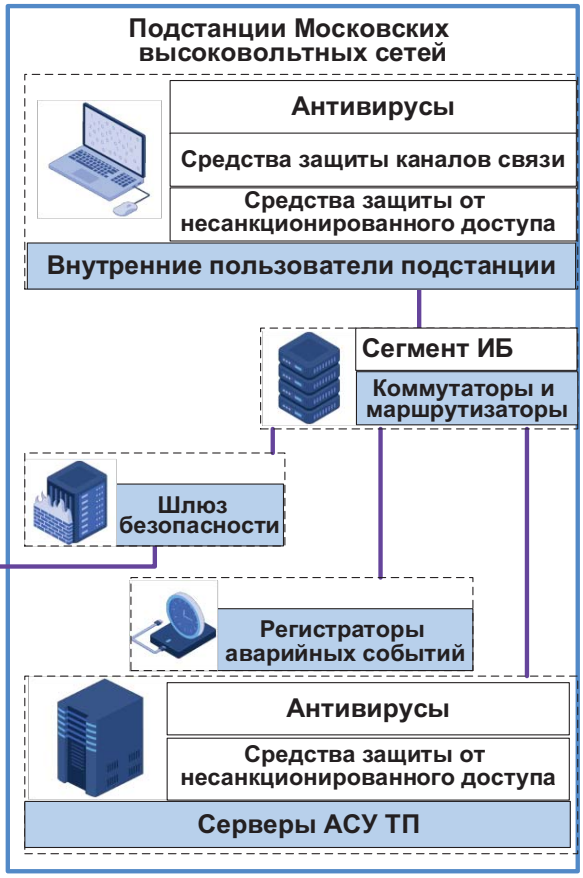


*Рис. 3. Схема защиты сегмента подстанций Московских высоковольтных сетей*

услуг в части информационной безопасности, но и, в первую очередь, их потребители. Так, в 2019 году ПАО «Россети Московский регион» в соответствии с Концепцией «Цифровая трансформация 2030» инициировало и реализует НИОКР «Организация цифрового дистанционного управления оборудованием и устройствами РЗА электрических распределительных устройств подстанций распределительных электрических сетей».

Основными целями НИОКР стали реализация цифрового защищенного дистанционного управления оборудованием и функциями РЗА из диспетчерского пункта ЦУС и диспетчерского центра РДУ, а также внедрение системы мониторинга устройств релейной защиты и автоматики на подстанциях 110–220 кВ. Создание системы мониторинга в защищенном исполнении позволяет обеспечить безопасное дистанционное управление с минимально возможными рисками несанкционированного воздействия на энергообъекты и выполнить требования по обеспечению безопасности в соответствии с законодательством РФ.

Построение вышеуказанной подсистемы защиты можно разделить между следующими условными сегментами:

– серверный сегмент филиала Московские высоковольтные сети ПАО «Россети Московский регион»;
– подстанции Московских высоковольтных сетей;
– удаленные (внешние) пользователи СРЗА.

В рамках построения подсистемы защиты, обеспечивающей безопасное дистанционное управление и мониторинг РЗА, были отдельно выделены сегменты информационной безопасности (сегменты ИБ), включающие в себя (в зависимости от конфигурации оборудования и типа контролируемой зоны) следующие виды средств защиты информации:

– средства защиты виртуальных сред;
– средства регистрации событий безопасности;
– средства анализа уязвимостей;
– средства обнаружения вторжений;
– средства защиты от несанкционированного доступа;
– средства анализа уязвимостей.

Часть элементов сегмента ИБ разворачивается на коммутаторах и маршрутизаторах, находящихся на границе защищаемого периметра.

В рамках серверного сегмента филиала Московские высоковольтные сети ПАО «Россети Московский регион» подсистема защиты реализуется согласно следующей схеме (рисунок 2).

Для подстанций Московских высоковольтных сетей реализуемая схема защиты несколько отличается (рисунок 3).

Защита внешних пользователей СРЗА реализуется при помощи средств антивирусной защиты, средств защиты от несанкционированного доступа и средств защиты каналов связи.

В общем виде взаимодействие между защищаемыми сегментами (рисунок 4) выглядит следующим образом:

– серверный сегмент и подстанции, обеспеченные средствами защиты информации на критических объектах и узлах, осуществляют информационное взаимодействие через шлюзы безопасности;

– внешние пользователи получают доступ к СРЗА посредством использования специального ПО, при помощи которого они имеют возможность подключаться к шлюзу безопасности серверного сегмента.

В ходе НИОКР были проведены работы по исследованию, проектированию и созданию подсистемы информационной безопасности для реализации защищенного дистанционного управления и мониторинга на подстанциях и в диспетчерском пункте Московских высоковольтных сетей — филиале ПАО «Россети Московский регион». Целями создания подсистемы информационной безопасности стали:

– минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности;
– предотвращение компьютерных атак в отношении объектов защиты;
– выполнение требований законодательства РФ в области защиты информации;
– обеспечение защищенности и устойчивого функционирования объектов защиты.

В соответствии с ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» и Приказом Министерства энергетики РФ от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования» на этапе проектирования было проведено предварительное категорирование, включающее в себя установление категории значимости информационной системы, и описание частной модели угроз, в соответствии с которой проводилась разработка подсистемы информационной безопасности для уровня подстанций и верхнего уровня ЦУС.

При разработке подсистемы информационной безопасности для уровня подстанций и верхнего уровня ЦУС был составлен перечень организационных и технических мероприятий в соответствии с ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».


*Рис. 4. Схема взаимодействия между защищаемыми сегментами*

Для оценки угроз использовались актуальные угрозы из «Банка данных угроз безопасности информации» ФСТЭК[1]. В дополнение к этому была проведена работа по анализу используемых компонентов и протоколов, обеспечивающих функционирование комплекса, в том числе рассматривались общеизвестные уязвимости (CVE[2]) с высоким рейтингом. По результатам проведенной работы было установлено, что используемые компоненты не имеют критичных уязвимостей. Исходя из полученной информации, была разработана модель подсистемы защиты информации, включающая технические меры по обеспечению безопасности в соответствии со следующими элементами:

– идентификации и аутентификации;
– управления доступом;
– защиты машинных носителей информации;
– аудита безопасности;
– антивирусной защиты;
– предотвращения вторжений;
– обеспечения целостности;
– защиты технических средств и систем;
– защиты системы и ее компонентов;
– реагирования на компьютерные инциденты.

Подсистема защиты информации (рисунок 5) обладает взаимосвязанными элементами, обеспечивающими комплексную защиту. Ниже представлена

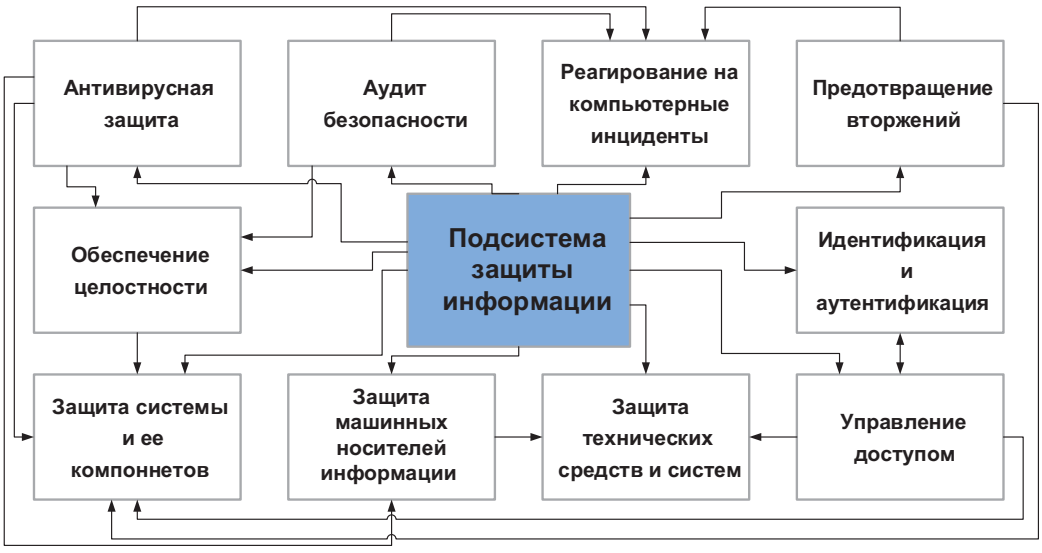


*Рис. 5. Структура подсистемы защиты информации*

[1] *ФСТЭК — Федеральная служба по техническому и экспортному контролю РФ.*

[2] *CVE — Common Vulnerabilities and Exposures. База данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.*

общая структура подсистемы защиты информации и взаимодействия ее элементов.

При проектировании подсистемы защиты информации очень важно внимательно подходить к вопросу совместимости наложенных средств защиты и проектируемых компонентов системы. Применяя сертифицированные средства защиты, можно столкнуться с риском невозможности использования последних версий операционных систем, баз данных, программных платформ (фреймворков) и иного ПО, необходимого для создания компонентов системы, в том числе из-за отсутствия поддержки новых версий сертифицированных средств защиты. Это вызвано тем, что процесс сертификации средств защиты весьма продолжителен по времени и ведет к значительным затратам для производителей. По этой причине внедрение новых сертифицированных версий продуктов происходит со значительной задержкой. Данные особенности необходимо учитывать как при разработке информационных систем любого типа, так и при разработке систем защиты информации. В случаях, когда предъявляются требования по использованию сертифицированных средств защиты, данные риски нужно учитывать и по отношению к архитектуре разрабатываемого программного продукта.

Следующий важный момент — необходимость обеспечения совместимости средств защиты информации с непрерывностью целостности промышленных процессов. В рамках НИОКР был создан специализированный полигон, на котором производилось тестирование влияния средств защиты информации на процессы дистанционного управления и мониторинга оборудования.

Для защиты каналов связи была реализована система шифрования VPN по алгоритму ГОСТ 28147-89: требование по обеспечению криптографической защиты каналов передачи сигналов управления является обязательным в соответствии с действующим законодательством. В ходе испытаний было установлено, что обмен информацией через шифрованный канал связи удовлетворяет требованию «…суммарное время на измерение и передачу телеметрической информации (ТИ, ТС) с объекта диспетчеризации в ДЦ устанавливается требованиями подсистем системы оперативно-диспетчерского управления, использующих эту информацию, и должно лежать в пределах не более 1–2 (одной-двух) секунд» (СТО 56947007-29.130.01.092-2011). Среднее значение, полученное в ходе испытаний, начиная с появления события и заканчивая его получением на стороне ДЦ, равнялось ~270 миллисекунд, среднее время на передачу информации через шифрованный канал — ~60 миллисекунд.

Роль криптошлюзов уровня подстанции выполняли аттестованные промышленные контроллеры, реализующие концепцию интеграции со средствами защиты (built-in-security). Контроллеры могут работать в суровых условиях эксплуатации, поддерживают шифрование по ГОСТу и совместимы с решениями от основных производителей средств криптозащиты. На платформе контроллеров функционирует сертифицированная подсистема обнаружения вторжений.

Преимущество использования предложенного подхода (концепция built-in-security) заключается в высокой надежности промышленной аппаратной платформы, в полной совместимости с решениями по автоматизации, снижении количества запасных изделий и приборов, а также компактном исполнении и низком энергопотреблении.

На тестовом полигоне было проведено обязательное тестирование внедренных средств защиты, относящихся к элементам подсистемы защиты информации: идентификации и аутентификации, управлению доступом, защите машинных носителей информации, аудиту безопасности, антивирусной защите, предотвращению вторжений, обеспечению целостности, защите технических средств и систем, защите системы и ее компонентов, реагированию на компьютерные инциденты. По результатам тестирования было установлено, что разработанное проектное решение по обеспечению информационной безопасности не оказывает негативного влияния на процессы мониторинга и дистанционного управления.

В дальнейшем, в рамках реализации проекта по внедрению, будет проведена аттестация защищаемой информационной системы на соответствие требованиям по защите информации.

## ВЫВОДЫ

В заключение следует сказать, что обеспечение информационной безопасности — итерационный, непрерывный процесс, в ходе которого происходит повторение таких действий, как анализ рисков и инцидентов, разработка мер по защите информации, их внедрение и проверка. Данные процессы рекомендуется регламентировать до начала эксплуатации системы, так как при эксплуатации необходимо обеспечить регулярность действий в соответствии с разработанной политикой информационной безопасности. В то же время защита информации должна осуществляться кадрами, обладающими достаточной компетенцией, образованием и профессиональной подготовкой.

Обеспечение информационной безопасности должно осуществляться для всех информационных систем защищаемого объекта: взлом любой из них, если те полностью не изолированы на физическом и логическом уровне, может повлечь за собой возможность проведения атаки нарушителем и дальнейшее распространение деструктивных воздействий. Данное правило особенно важно к выполнению для взаимодействующих систем.

При дальнейшем масштабировании или тиражировании технологии дистанционного управления и мониторинга оборудования необходимо проводить регулярный анализ угроз. При этом должны быть учтены не только угрозы из банка угроз ФСТЭК, но и те, что размещены в иных открытых источниках (например, MITRE CVE и база данных NVD).

С целью выполнения требований по информационной безопасности и конфиденциальности в статье не приводилось детального описания средств защиты, их настроек и схемы взаимодействия средств защиты информации и информационных систем.

ЛИТЕРАТУРА

1. Сборник тезисов XXVII международная научно-техническая конференция «Радиоэлектроника, электротехника и энергетика». М.: ООО «Центр полиграфических услуг «Радуга», 2020. 1158 с.
2. Ландшафт угроз для компьютеров, используемых для инжиниринга и интеграции АСУ ТП. 2020. URL: https://ics-cert.kaspersky.ru/reports/2021/03/17/threat-landscape-for-the-ics-engineering-and-integration-sector-2020/.
3. Карантаев В.Г., Карпенко В.И. Анализ нарушений работоспособности объектов электроэнергетики вследствие кибератак / Connect 2020 г. URL: https://www.connect-wit.ru/analiz-narushenij-rabotosposobnosti-obektov-elektroenergetiki-vsledstvie-kiberatak.html.
4. Плешко Д.Ю. Влияние кибербезопасности объектов электроэнергетики на надежность функционирования ЭЭС // Актуальные проблемы энергетики, 2017. С. 564–567.

REFERENCES

1.
2. URL: https://ics-cert.kaspersky.ru/reports/2021/03/17/threat-landscape-for-the-ics-engineering-and-integration-sector-2020/.
3. URL: https://www.connect-wit.ru/analiz-narushenij-rabotosposobnosti-obektov-elektroenergetiki-vsledstvie-kiberatak.html.
4.