УДК 004.056.53

С. П. Серёдкин, Е. В. Бердникова

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ В ТЕХНОЛОГИЧЕСКОМ И КОРПОРАТИВНОМ СЕГМЕНТАХ СЕТИ С ИСПОЛЬЗОВАНИЕМ ДИОДОВ ДАННЫХ

Аннотация. *В работе рассмотрена технология «Диод данных», позволяющая обеспечить требуемый уровень информационной безопасности промышленных систем. Использование технологии однонаправленного диода данных дает возможность повысить уровень защищенности критически важных цифровых систем, промышленных объектов управления от входящих кибератак. Кроме того в работе исследуется проблема безопасности промышленных систем с применением диода данных и предлагаются схемы их эффективного использования в сетях управления технологическими процессами.*

Ключевые слова: *Data Diode (диод данных), автоматизированные системы управления технологическими процессами, безопасность на объектах критической информационной инфраструктуры, защита информации, кибербезопасность.*

S. P. Seredkin, E. V. Berdnikova

Irkutsk State Transport University, Irkutsk, the Russian Federation

IMPROVING SECURITY IN THE TECHNOLOGICAL AND CORPORATE NETWORK SEGMENTS USING DATA DIODES

Abstract. *The work discusses the "Data Diode" technology, which allows ensuring the required level of information security of industrial systems. The use of unidirectional data diode technology makes it possible to increase the level of security of critical digital systems and industrial control facilities from incoming cyber-attacks. In addition, the work examines the problem of security of industrial systems using a data diode and proposes schemes for their effective use in process control networks.*

Keywords: *data diode, automated process control systems, security at critical information infrastructure facilities, information protection, cybersecurity.*

Введение

В сфере кибербезопасности существует значительное количество векторов атак и средств (таких как вложения электронной почты, всплывающие окна, обман, чаты, вирусы, USB-накопители, удаленный доступ и т.д.), с помощью которых злоумышленники могут нарушить конфиденциальность, целостность и доступность сети и данных [1]. Доступ к сети может быть принудительным с целью изменения или нарушения ее работы, удаления данных или их использования в незаконных целях. Все эти нарушения могут привести к значительному ущербу для объекта атаки [2]. В промышленном Интернете вещей (IIoT) эти векторы атак на кибербезопасность представляют собой проблему для чувствительных, дорогостоящих сетей, которые должны оставаться защищенными и в то же время открытыми для предоставления и интеграции потоков данных авторизованных пользователей.

Общепринятой стратегией кибербезопасности является внедрение многоуровневого подхода к обеспечению информационной безопасности методом разделения или сегментации областей, которые имеют разные уровни доверия [3]. Существует множество средств защиты сетей от внешних угроз, таких как брандмауэры (программные), автономные сети (физические) или каналы передачи данных (аппаратные). У каждого из них есть свои достоинства и недостатки, которые, в свою очередь, не всегда являются эффективными при определенных условиях [4].

История технологии «Диод данных»

Как уже сказано выше, существуют три фундаментальные цели, которыми руководствуется политика кибербезопасности внутри организации [5]:

- конфиденциальность: обеспечение того, чтобы конфиденциальная информация не передавалась тем, у кого нет к ней доступа;
- целостность: поддержание согласованности, точности и достоверности данных на протяжении всего их жизненного цикла;
- доступность: обеспечение доступности данных без каких-либо сбоев, таких как поддержание резервной копии файлов и обеспечение достаточной полосы пропускания для авторизированных пользователей.

Технология «Диод данных» может обеспечить кибербезопасность и в то же время обеспечить подключение к сети. Информационные диоды традиционно служат для защиты конфиденциальных данных и активов. Когда для защиты информации используется диод данных, конфиденциальность имеет приоритет над целостностью. Когда защита активов (как правило, промышленных систем) является основной целью - целостность и доступность имеют важное значение.

Развитие технологии «Диод данных» началось еще во второй половине 20 века, однако практическое применение относится к началу 21 века. Википедия определяет его как сетевое устройство, позволяющее передавать данные только в одном направлении. Передача данных в обратном направлении невозможна из-за физических свойств диода.

Одним из примеров является использование этой технологии в российских государственных информационных системах, где доступ в Интернет запрещен, однако потребность в использовании Интернета остается высокой, включая обновление программного обеспечения и поиск информации. Другой пример - необходимость передачи информации между сетями с разной степенью секретности, такой как передача информации из сетей, обрабатывающих документы с ограниченным доступом, в сети с более высоким уровнем секретности. Физические ограничения доступа часто приводят к передаче информации на физических носителях, что увеличивает риск внедрения вредоносного кода.

Актуальность данной технологии

Как уже говорилось ранее, диоды данных обеспечивают физический механизм для обеспечения строго однонаправленной связи между двумя сетями, исключая возможность утечки информации из внутренней сети или внедрения вредоносного кода путем проверки получаемых данных [6]. В качестве аналогии можно привести обычное радио: мы можем настроиться на любую радиостанцию, но не можем ничего передать. По такому же принципу работает диод данных - у него физически отсутствует передатчик информации. Как это достигается?

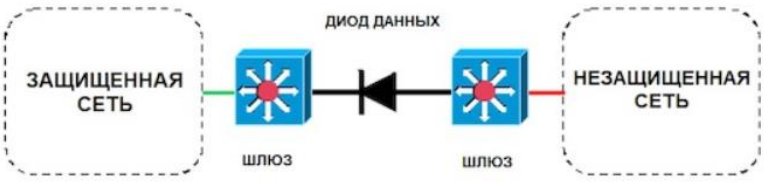

Рис. 1. – Концепция работы диода данных

Помимо государственных ИС однонаправленная передача данных необходима и в объектах критической информационной инфраструктуры (далее ОКИИ) [7]. Для обеспечения

безопасности на ОКИИ необходимо соблюдение требований следующих нормативно-правовых актов (далее НПА): Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ, приказы ФСТЭК России № 235, 236 и 239, а также указы Президента РФ № 166 и 250. Как показывает практика, при выполнении требований данных НПА у организаций возникают вопросы и сложности, связанные с особенностями производственных объектов, технологических процессов и систем, которые их обеспечивают. Например, необходимо разделение сетей при использовании автоматизированной системы управления технологическими процессами (рис. 2).

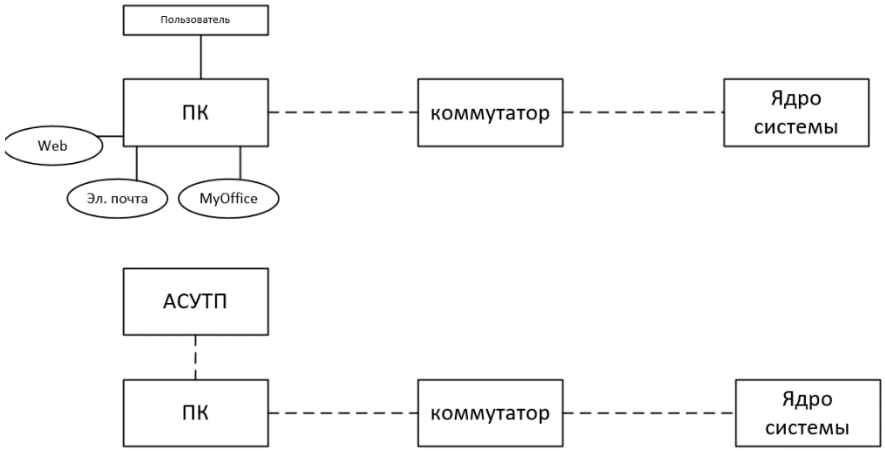

Рис. 2. – Схема реализации защищенной сети, предусматривающая физическое разделение

Для упрощения этой схемы и уменьшения затрат организации на дополнительное оборудование и применяется диод данных, который передает информацию из АСУТП, но при этом исключает управление данной системой (рис. 3).

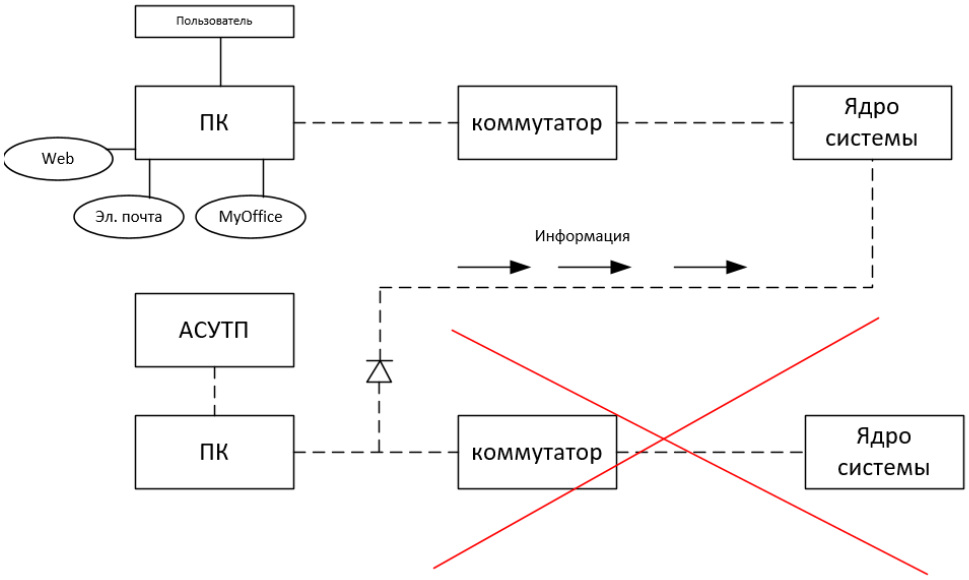

Рис. 3. – Схема реализации защищенной сети, предусматривающая использование диода-данных

Сильные и слабые стороны технологии Data Diode

Наиболее сильной особенностью технологии data diode, является ее аппаратный аспект. Благодаря этой технологии нет памяти, настроек или параметров, которые можно было бы изменить или взломать, что придает программным решениям присущие им недостатки. Существуют версии диодов данных, доступные со встроенными программными компонентами, которые уязвимы для атак. В этом смысле не все информационные диоды одинаковы [8].

Благодаря использованию аппаратной системы обе конфигурации информационных диодов в значительной степени исключают возможность ошибки пользователя. Например, хотя брандмауэр может защитить сами данные от повреждения, он не защищает от того, что пользователь «запускает» вредоносное ПО, которое может раскрыть информацию в сети с высоким уровнем безопасности. Информационные диоды просто предотвращают возникновение такой возможности.

Еще одним преимуществом, вытекающим из их аппаратного компонента, является способность диодов данных, предназначенных только для передачи, защищать и сохранять устаревшие системы. Многие системы, управляющие критически важной инфраструктурой, работают на более устаревшем оборудовании. С помощью диодов данных можно защитить устаревшие системы без модернизации операционной системы. Это значительное преимущество, поскольку эти системы, как правило, создаются постепенно в течение нескольких лет и прерывание их работы не допустимо в условиях непрерывности производства.

Применимость технологии data diode выходит за рамки критически важной инфраструктуры. Многие избирательные системы работают на старом программном обеспечении и оборудовании, что делает их уязвимыми для кибератак. Внедряя информационные диоды в такого рода устаревшие системы, можно повысить безопасность системы без необходимости переводить их в автономный режим или аналогичным образом обновлять и, возможно, подвергать при этом большему количеству уязвимостей.

Не менее важно, что третье преимущество диодов, предназначенных как для передачи, так и для приема данных, заключается в их способности обеспечивать безопасность в небезопасных системах. Хакеры выбирают для атаки сетевые системы в зависимости от того, какого рода слабые места они представляют. Двумя наиболее распространенными типами кибератак являются DDoS-атаки и перегрузка буфера. DDoS-атаки основаны на двустороннем трафике и поэтому недоступны хакерам, желающим проникнуть в систему, предназначенную только для передачи данных. В конфигурации только для приема диоды данных должны были бы полагаться на установленное программное обеспечение, которое отметило бы такую атаку как нерегулярную, или было бы ограничение потока данных, которыми обладают некоторые диоды [9].

Высокая стоимость представляет собой одну из самых больших проблем при внедрении технологий передачи данных. В России больший спрос имеют отечественные производители, так по требованию приказов ФСТЭК №17,21,31 средства защиты должны быть сертифицированы ФСТЭК России с указанием уровня контроля, получить такую сертификацию на зарубежные системы довольно сложно.

Кроме того, для установки информационных диодов требуются специальные знания и навыки, которыми клиенты не всегда обладают (установка информационных диодов может занять до двух дней). Настройка и мониторинг также могут привести к увеличению затрат и усложнению эксплуатации устройства для пользователя, что снижает спрос со стороны предприятий, не имеющих квалифицированного персонала для выполнения работ в сфере информационных технологий и защиты информации.

Еще одна проблема, связанная с использованием технологии data diode, заключается в том, что подавляющее большинство современных коммуникационных протоколов для функционирования требуют двусторонней связи. Диоды передачи данных не работают со стандартными протоколами TCP/IP, только с протоколами, которые являются однонаправленными по своей конструкции, и которые не требуют подтверждения получения. По причине реализации протокола передача некоторого типа данных может быть медленной и недостаточно надежной. Данные, передаваемые по каналу передачи данных, должны быть тщательно от-

фильтрованы, поскольку объем данных, которые могут быть отправлены, ограничен. Кроме того, диоды, предназначенные только для передачи данных, не могут считывать, были ли данные успешно получены, что может привести к затруднению информационных потоков и потере данных [10].

Заключение

Внедрение технологии Диод данных началось во второй половине 20-го века, более широкое практическое применение информационных диодов относится к началу нынешнего столетия. Исторически сложилось так, что применение данной технологии ограничивалось военным и оборонным секторами. Промышленные системы управления представляют собой в настоящее время развивающийся рынок. С учетом объективных факторов в последние два-три года технологии передачи данных на диодах уделяется повышенное внимание. Одним из наиболее привлекательных компонентов является его физическое измерение в обеспечении безопасности. В современных условиях возросшего количества кибератак на информационную инфраструктуру информационные диоды являются ценным потенциальным дополнением к существующему набору инструментов кибербезопасности.

На данный момент внимание сконцентрировано, в первую очередь, на секторе высокого риска: функционировании критически важной инфраструктуры и защите секретных информационных систем. Любой сбой или нарушение в рамках этого сектора может привести к значительному ущербу на государственном уровне, тем самым представляя угрозу национальной безопасности.

Технология Data Diode в настоящее время всё шире применяется именно как инструмент повышения уровня информационной безопасности для государственных структур и бизнеса в интересах обеспечения национальной безопасности государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ларин Д. А. Информационная безопасность. История защиты информации в России / Д. А. Ларин. – Москва : КДУ, 2015. – 736 с.

2. Информационная безопасность / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – Москва : ТИД ДиаСофт, 2016. – 537 с

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. – Москва : ФОРУМ, 2022. – 416 с.

4. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации. Учебное пособие. / А.А. Малюк. – Москва : Горячая Линия - Телеком, 2017. – 280 с.

5. Поляков, В.С. Комплексная защита информации в компьютерных системах и сетях / В.С. Поляков, А.В Сулимов. – Москва : БХВ-Петербург, 2021. – 544 с.

6. Шаньгин, в. ф. Комплексная защита информации в корпоративных системах / в. ф. Шаньгин. – Москва : ФОРУМ, 2022. – 592 с.

7. Концепция совершенствования кибербезопасности критически важной инфраструктуры - Дополнительные материалы к докладу на конференции «IT Security Conference 2019» // Перевод. г. Минск, 2019. – 64 с

8. Прокопенков В.И., Колесников А.А., Тезин А.В. Алгоритм применения программных и аппаратно-программных средств для организации защищенного обмена с внешними информационными системами, исключающий утечку информации ограниченного доступа (вариант однонаправленных шлюзов) // СТУДЕНЧЕСКИЙ ВЕСТНИК Учредители: Общество с ограниченной ответственностью "Интернаука". - 2022. - №23-10 (215) . - С. 23-26.

9. Воронцов А.Г., Петунин С.А. Организация однонаправленных сетей передачи информации в условиях защищённой среды // Вопросы кибербезопасности Учредители: Научно-производственное объединение Эшелон ISSN: 2311-3456. - 2017. - №2 (20) . - С. 21-29.

10. Куракин А.С. Опыт применения средств однонаправленной передачи данных для сопряжения закрытого и открытого сегментов сети // Информационная безопасность - актуальная проблема современности. совершенствование образовательных технологий подготовки специалистов в области информационной безопасности Учредители: Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. - 2019. - №1 (10) . - С. 219-221.

REFERENCES

1. Larin D. A. Informatsionnaia bezopasnost'. Istoriia zashchity informatsii v Rossii / D. A. Larin. – Moskva : KDU, 2015. – 736 p.

2. Informatsionnaia bezopasnost' / S. V. Zapechnikov, N. G. Miloslavskaia, A. I. Tolstoi, D. V. Ushakov. – Moskva : TID DiaSoft, 2016. – 537 s

3. SHan'gin V.F. Informatsionnaia bezopasnost' komp'iuternykh sistem i setei / V.F. SHan'gin. – Moskva : FORUM, 2022. – 416 p.

4. Maliuk A.A. Informatsionnaia bezopasnost'. Kontseptual'nye i metodologicheskie osnovy zashchity informatsii. Uchebnoe posobie. / A.A. Maliuk. – Moskva : Goriachaia Liniia - Telekom, 2017. – 280 p.

5. Poliakov, V.S. Kompleksnaia zashchita informatsii v komp'iuternykh sistemakh i setiakh / V.S. Poliakov, A.V Sulimov. – Moskva : BKHV-Peterburg, 2021. – 544 p.

6. SHan'gin, v. f. Kompleksnaia zashchita informatsii v korporativnykh sistemakh / v. f. SHan'gin. – Moskva : FORUM, 2022. – 592 p.

7. Kontseptsiia sovershenstvovaniia kiberbezopasnosti kriticheski vazhnoi infrastruktury - Dopolnitel'nye materialy k dokladu na konferentsii «IT Security Conference 2019» // Perevod. g. Minsk, 2019. – 64 s

8. Prokopenkov V.I., Kolesnikov A.A., Tezin A.V. Algoritm primeneniia programmnykh i apparatno-programmnykh sredstv dlia organizatsii zashchishchennogo obmena s vneshnimi informatsi-onnymi sistemami, iskliuchaiushchii utechku informatsii ogranichennogo dostupa (variant odnona-pravlennykh shliu-zov) // STUDENCHESKII VESTNIK Uchrediteli: Obshchestvo s ogranichennoi otvetstvennost'iu "Internauka". - 2022. - no23-10 (215) . - S. 23-26.

9. Vorontsov A.G., Petunin S.A. Organizatsiia odnonapravlennykh setei peredachi informatsii v usloviiakh zashchishchënnoi sredy // Voprosy kiberbezopasnosti Uchrediteli: Nauchno-proizvodstvennoe obedinenie Eshelon ISSN: 2311-3456. - 2017. - no2 (20) . - S. 21-29.

10. Kurakin A.S. Opyt primeneniia sredstv odnonapravlennoi peredachi dannykh dlia sopriazheniia zakrytogo i otkrytogo segmentov seti // Informatsionnaia bezopasnost' - aktual'naia problema sovremennosti. sovershenstvovanie obrazovatel'nykh tekhnologii podgotovki spetsialistov v oblasti informatsionnoi bezopasnosti Uchrediteli: Krasnodarskoe vysshee voennoe uchilishche im. generala armii S.M. SHtemenko. - 2019. - no1 (10) . - S. 219-221.

Информация об авторах

Серёдкин Сергей Петрович - к.э.н. доцент кафедры ИСиЗИ, Иркутский государственный университет путей сообщения, г. Иркутск

Бердникова Екатерина Васильевна - студент группы БИм.1-22-1, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: just_katrin777@mail.ru

Information about the authors

Seredkin Sergey Petrovich – candidate of technical Sciences,Associate Professor,Associate Professor of the Department "Information systems and information protection", Irkutsk State Transport University, Irkutsk

Lisitsyn Vladislav Alexandrovich – student of the BIm group.1-22-1, Irkutsk State Transport University, Irkutsk