3. Шаньгин В. Ф. Защита в компьютерных системах и сетях / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2012. – 592 с.

4. Fujioka A. A practical secret voting scheme for large scale election / A. Fujioka, T. Okamoto and K. Ohta // Advances in Cryptology-Auscrypt'92, LNCS 718. – Springer-Verlag, 1992. – P. 244–260.

5. Announcing the Advanced Encryption Standard (AES). – Federal Information Processing Standards Publication 197, 2001.

6. Chaum D. Blind signatures for untraceable payments / D. Chaum // Proceedings of Crypto 82. – New York : Plenum Press, 1983. – P. 199–203.

7. Nurmi H. Secret ballot elections in computer networks / H. Nurmi, A. Salomaa, L. Santean // Computers and Security. – 1991. – Vol. 36, № 10. – P. 553–560.

8. RFC 2818 HTTP over TLS. – 2000.

9. Rivest R. L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems / R. L. Rivest, A. Shamir, L. M. Adleman Communications of the ACM. – 1978. – Vol. 21, № 2. – P. 120–126.

10. RSA Laboratories. PKCS #1 v2.2: RSA Cryptography Standard. – 2012.

11. Shamir A. Comm. of the ACM / A. Shamir. – 1979. – Vol. 22. – P. 612.

References

1. Shnayer. B. *Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si* [Applied Cryptography. Protocols, algorithms, sources in C++]. Moscow, Triumf Publ., 2002. 815 p.

2. Mao V. *Sovremennaya kriptografiya. Teoriya i praktika* [Modern cryptography. Theory and practice]. Moscow, Vilyams Publ., 2005. 763 p.

3. Shangin V. F. *Zashchita v kompyuternykh sistemakh i setyakh* [Security in computer systems and networks]. Moscow, DMK Press Publ., 2012. 592 p.

4. Fujioka A., Okamoto T. and Ohta K. A practical secret voting scheme for large scale election. *Advances in Cryptology-Auscrypt'92, LNCS 718*. Springer-Verlag, 1992, pp. 244–260.

5. *Announcing the Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197, 2001.

6. Chaum D. Blind signatures for untraceable payments. *Proceedings of Crypto 82*. New York, Plenum Press, 1983, pp. 199–203.

7. Nurmi H., Salomaa A., Santean L. Secret ballot elections in computer networks. *Computers and Security*, vol. 36, no. 10, 1991, pp. 553–560.

8. RFC 2818 HTTP over TLS, 2000.

9. Rivest R. L., Shamir A., Adleman L. M. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120–126.

10. *RSA Laboratories, PKCS #1 v2.2: RSA Cryptography Standard*, 2012.

11. Shamir A. *Comm. of the ACM*, 1979, vol. 22, p. 612.

УДК 004.056
DOI 10.21672/2074-1707.2019.47.3.102-121

АНАЛИЗ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП ГАЗОДОБЫВАЮЩИХ ПРЕДПРИЯТИЙ

Статья поступила в редакцию 10.06.2019, в окончательном варианте – 26.08.2019.

Римша Андрей Сергеевич, Тюменский государственный университет, 625003, Российская Федерация, г. Тюмень, ул. Перекопская, 15А,

аспирант, e-mail: RimshaAndrew@gmail.com

Римша Константин Сергеевич, Тюменский государственный университет, 625003, Российская Федерация, г. Тюмень, ул. Перекопская, 15А,

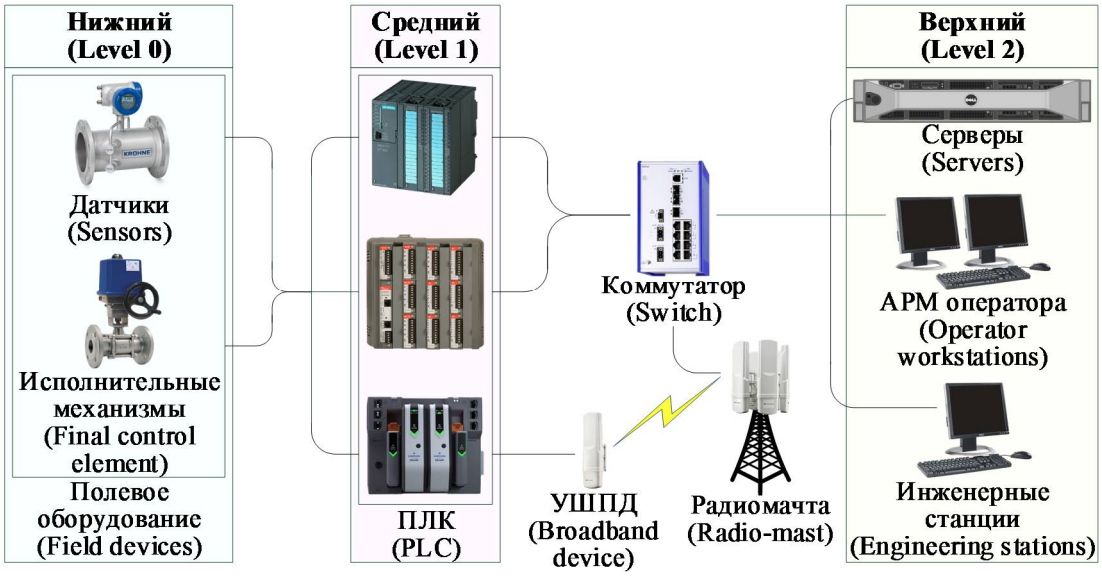
студент, e-mail: RimshaKonstantin@ya.ru

Цели исследования, описанного в данной статье: анализ актуальных классов решений для обеспечения информационной безопасности АСУ ТП газодобывающего предприятия; выбор наиболее подходящего решения и сравнение его с используемыми на рынке решениями соответствующего класса; формирование нового подхода к моделированию угроз; разработка программной реализации для предложенного раннее метода оценки угроз. Для достижения поставленных целей решен ряд научных задач. Проведено исследование нескольких средств информационной безопасности с учетом опыта их применения в автоматизированных системах; установлены критерии для сравнения рассматриваемых решений; в результате было определено средство, по своим характеристикам в наибольшей степени удовлетворяющее критериям сравнения. Рассмотрены популярные решения, относящиеся к данному классу, их достоинства и недостатки. Учитывая специфические особенности обеспечения информационной безопасности АСУ ТП, были сформулированы определенные требования, причем ни одно из рассмотренных решений в полной

мере не удовлетворило указанным требованиям. Поэтому был разработан программный комплекс для моделирования угроз и оценки рисков информационной безопасности, удовлетворяющий сформулированным требованиям. В статье описан интерфейс этого комплекса. Указанный комплекс позволяет выполнить комплексное моделирование угроз и оценить риски информационной безопасности АСУ ТП газодобывающих предприятий.

Ключевые слова: автоматизированная система управления, информационная безопасность, средства защиты информации, газодобывающее предприятие, средства моделирования угроз, оценка рисков, идентификация уязвимостей, программный комплекс

Графическая аннотация (Graphical annotation)



ANALYSIS OF INFORMATION SECURITY' TOOLS FOR APCS OF GAS PRODUCING ENTERPRISES

The article was received by the editorial board on 10.06.2019, in the final version – 26.08.2019.

Rimsha Andrew S., Tyumen State University, 15A Perekopskaya St., Tyumen, 625003, Russian Federation,

graduate student, e-mail: RimshaAndrew@gmail.com

Rimsha Konstantin S., Tyumen State University, 15A Perekopskaya St., Tyumen, 625003, Russian Federation,

student, e-mail: RimshaKonstantin@ya.ru

The objectives of the study described in this article are an analysis of the actual classes of information security solutions for the APCS of gas producing enterprise; a selection of the most appropriate class of solution and comparison of representatives of this class used in the market; a formation of a new approach to threat modeling; the development of an information security risk assessment methodology; the development of software implementation for this methodology. To achieve these goals, several scientific problems have been solved. A study of several information security tools was carried out considering their use in automated systems; established criteria for comparing the considered decisions, as a result, the tool was determined according to its characteristics that best meet the comparison criteria; the popular solutions of this class listed, considering their advantages and disadvantages. Considering the specific features of providing information security for APCS, certain requirements are formed, not one of these solutions did not fully satisfy these requirements. Consequently, the proposed methodology for modelling threats and assessing the risks of information security that meets the requirements; describes the interface and the possibility of the software implementation of the proposed methodology. The developed program allows you to simulate threats and assess the risks of information security of APCS of gas producing enterprises.

Keywords: APCS, information security, information security tools, gas producing enterprise, threat modeling tools, risk assessment, vulnerability identification, software package

Введение. Автоматизированная система управления (АСУ) технологическими процессами (ТП) – это целая группа технических и программных средств, предназначенных для автоматизации процессов управления технологическим оборудованием на промышленных предприятиях. Серьезной угрозой для таких предприятий сегодня является возможность вмешательства террористических, экстремистских и враждебно настроенных групп в управление АСУ критически важных объектов, в том числе и с целью вывода их из строя.

Важным направлением для корректного функционирования АСУ ТП является обеспечение информационной безопасности (ИБ) этих систем. Отрасли, где защита АСУ ТП наиболее критична, те, в которых возможен максимальный ущерб и может пострадать наибольшее количество людей и оборудования, – это энергетические компании и предприятия топливно-энергетических комплексов (ТЭК). Здесь возможны как негативные экономические последствия, например, нарушение поставок нефти или газа или перебои в электроснабжении населения, так и экологические или гуманитарные катастрофы.

Одним из наиболее опасных видов деятельности в сфере ТЭК является добыча газа. Его физические и химические свойства накладывают повышенные требования в отношении обеспечения промышленной безопасности предприятий. В настоящее время Россия обладает самыми крупными запасами природного газа в мире. При таких условиях помимо «промышленной безопасности» необходимо обеспечение гарантированного уровня ИБ газодобывающих предприятий (ГДП), что требует совершенствования систем, средств и процессов управления ИБ. Эти вопросы в существующих публикациях разработаны недостаточно полно.

В связи с этим целью данной работы стал анализ существующих средств обеспечения ИБ АСУ ГДП.

Для достижения поставленной цели необходимо решить следующие задачи:

- описать процесс работы типовых АСУ ТП;
- рассмотреть основные типы нарушений ИБ в АСУ ТП;
- рассмотреть и сравнить актуальные средства обеспечения ИБ АСУ ТП ГДП;
- выбрать средство обеспечения ИБ АСУ ТП ГДП и обосновать целесообразность его использования.

Общая характеристика проблематики исследований. Под «промышленной безопасностью» подразумевается обеспечение для оборудования безопасных режимов функционирования, предотвращающих ускоренный износ оборудования, а также снижение возможных негативных влияний людей-операторов на процессы управления (с целью сокращения аварийных остановок оборудования, предотвращения сверхнормативных вредных выбросов в воздух и пр.).

Под «управлением» в статье понимается процесс изменения состояния или режима функционирования системы в соответствии с поставленной перед ней задачей [3]. Исходя из этого определения, управление направлено на то, чтобы целенаправленно менять состояние системы.

Для обеспечения ИБ АСУ ТП ГДП необходимо рассмотреть, что из себя представляют системы автоматического управления (САУ) таких предприятий.

Рассмотрим процесс управления на примере ГДП. Пусть технологическая установка по добыче газа является объектом управления, а САУ – органом (средством) управления. В таком случае САУ формирует управляющее воздействие на исполнительные механизмы, установленные на скважинах, которые открывают (регулируют) или перекрывают потоки газа, а технологическая установка формирует обратную связь, отправляя сигналы с датчиков. На основании обратной связи САУ может корректировать свои управляющие воздействия. Таким образом, в данной системе не принимает участие человек, и она является замкнутой. [3]. Основная особенность САУ в том, что в таких системах происходит очень быстрый анализ «информации обратной связи» при формировании сигналов управления. Из-за больших объемов информации и необходимости быстрых реакций на нее человек не способен достаточно быстро принимать и реализовывать правильные решения, т.е. заменить САУ. На рисунке 1 представлена схема САУ.

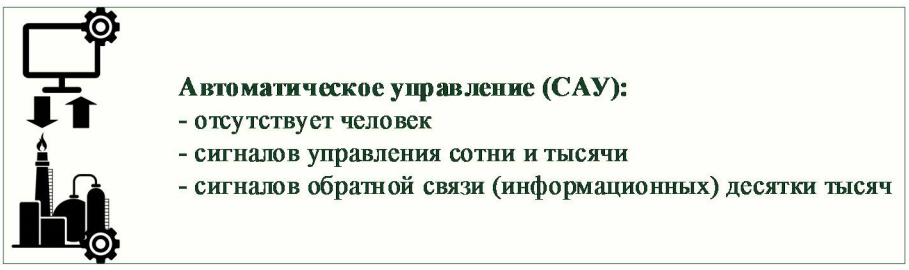


Рисунок 1 – Система автоматического управления [6]

Система, в которой человек участвует в принятии и реализации решений по управлению ТП, относятся к классу АСУ ТП. При этом важно понимать, что возможности человека по обработке информации ограничены, поэтому он может участвовать в принятии и реализации только некоторых видов решений. Для управления в рамках АСУ и, в частности, снижения объемов поступающей информации, используется преобразующий интерфейс. С его помощью на экране демонстрируются показания приборов, где человек может проверить: соответствуют ли данные получаемые с датчиков действительности или нет. Таким образом, через АСУ человек может оказывать воздействие на объект управления, однако это воздействие не прямое, а косвенное. Косвенное воздействие характерно тем, что результат воздействия и сигналы обратной связи могут не совпадать, поэтому операторам необходимо проверять фактическое выполнение некоторых действий вручную. На рисунке 2 представлена схема АСУ ТП.

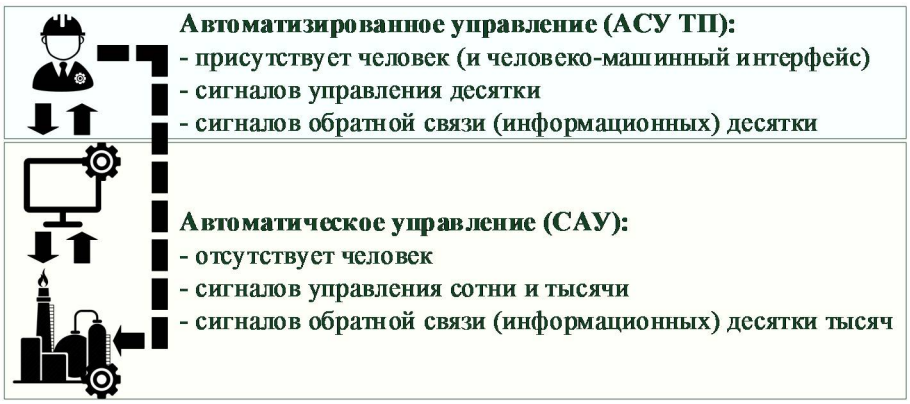


Рисунок 2 – Автоматизированная система управления технологическими процессами [6]

Типовое ГДП представляет собой территориально распределенную структуру, которая начинается от кустов газовых скважин и заканчивается центральным диспетчерским пунктом. Как правило, в промышленных АСУ ТП выделяют три уровня [9]:

- нижний уровень – уровень датчиков и исполнительных механизмов;
- средний уровень – уровень программируемых логических контроллеров (ПЛК);
- верхний уровень – система сбора данных и оперативного диспетчерского управления (англ. SCADA – Supervisory Control And Data Acquisition).

Объединение устройств АСУ ТП в сеть, наличие соединений между различными зонами, а также появление интерфейсов для удаленного обслуживания создают условия, при которых возникают угрозы ИБ для АСУ ТП и предприятия в целом. Связь между компонентами АСУ ТП, уязвимостями и угрозами представлена в виде трехдольного графа [1] на рисунке 3.

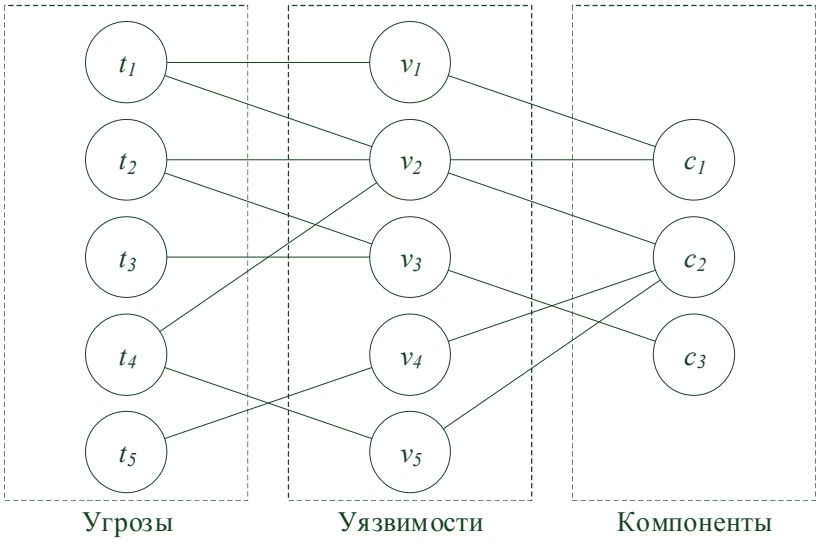


Рисунок 3 – Связь между компонентами, уязвимостями и угрозами

Федеральным законом РФ от 26 июля 2017 г. № 187-ФЗ информационные системы, информационно-телекоммуникационные сети, АСУ, функционирующие в сфере ТЭК, отнесены к субъектам критической информационной инфраструктуры. Поэтому к системам автоматизации предприятий ТЭК предъявляются повышенные требования по обеспечению стабильности работы, надежности функционирования оборудования. Эти требования обусловливают наличие особого подхода при построении и поддержании системы защиты информации АСУ ТП ГДП от реально существующих и потенциально возможных угроз ИБ.

Основные типы угроз и нарушений ИБ в АСУ ТП. Типы угроз ИБ очень разнообразны и имеют множество классификаций [5]. Однако, учитывая специфику рассматриваемых АСУ ТП, были выделены следующие три основных типа нарушений ИБ.

1. Пренебрежение и халатность со стороны собственных работников предприятия. Подобные инциденты возникают в случае использования производственной инфраструктуры не по назначению. Например, подключение внешних устройств (носители информации, модемы и другие), установка незадекларированного программного обеспечения (ПО) или подключение сторонних средств вычислительной техники (СВТ) в промышленную сеть.

2. Хищения. В отличие от предыдущего типа нарушений этот тип является умышленным и подразумевает использование АСУ ТП для того, чтобы скрывать хищения сырья, например, газа или конденсата.

3. Целевая кибератака (или Advanced Persistent Threat (APT)). Такой тип нарушений ИБ направлен на использование АСУ ТП с целью повлиять на производственные процессы предприятия [11]. Это влияние может быть либо промышленным шпионажем (чтобы получить конфиденциальные данные), либо саботажем, направленным на прекращение производственного процесса или повышение вероятности возникновения аварийных ситуаций.

Далее эти три направления рассматриваются более подробно с учетом АСУ ТП ГДП.

Пренебрежение правилами и халатность со стороны собственных работников предприятия. Ненадлежащее выполнение (или невыполнение) работниками предприятия правил в сфере ИБ может привести к серьезным последствиям, которые могут повлиять на технологический процесс ГДП.

1. Примерный типичный сценарий нарушения ИБ: оператор подключил съемный носитель, зараженный вредоносным ПО, к автоматизированному рабочему месту (АРМ). В случае отсутствия антивирусов или использования их устаревших баз скриптов вредоносное ПО проникает на клиентскую машину оператора, нарушая при этом ее работу, и имеет потенциальную возможность распространиться на остальные устройства в локальной сети.

Одним из вариантов проявления действий вредоносного ПО могут быть ошибки операционной системы (ОС), связанные с недостатком системных ресурсов для выполнения операций. Также популярным типом вредоносного ПО являются вирусы-вымогатели, которые поражают АРМ или сервера, блокируя доступ к ОС или предотвращают считывание записанных данных, требуя у жертвы выкуп для восстановления исходного состояния системы.

2. Второй сценарий нарушения ИБ подразумевает подключение устройств, выполняющих функцию модема, к АРМ с доступом в SCADA-систему. Таким образом, это устройство оказывается в глобальной сети и оказывается подверженным множеству потенциальных угроз. Примером такой атаки может стать скрытно устанавливаемая на АРМ-оператора программа, позволяющая злоумышленнику выполнять действия с использованием ресурсов зараженной машины. Одним из таких действий может быть DoS-атака (Denial of Service) на устройства внутри промышленной сети.

Еще одним потенциально возможным подвариантом может быть нарушение отображения информации, используемой оператором АСУ ТП для принятия и реализации оперативных решений. В этих случаях из-за неверной информации операторами могут приниматься и выполняться неверные решения, которые могут приводить к аварийным ситуациям.

В формализованном виде примеры сценариев нарушения ИБ (и их последствия) вследствие пренебрежения и халатности со стороны собственных работников представлены на рисунке 4.

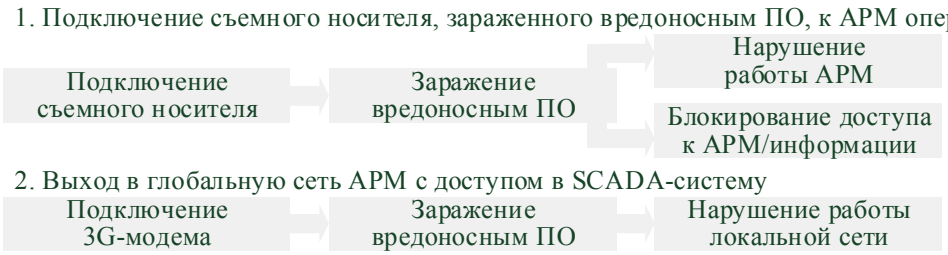


Рисунок 4 – Сценарии нарушения ИБ вследствие халатности со стороны собственных работников

Отметим, что в силу специфики работы ГДП и их АСУ даже кратковременные однократные неблагоприятные воздействия вредоносных программ могут иметь весьма неблагоприятные последствия для организаций, их подразделений.

Хищение. Информация о том, сколько было добыто ресурсов во время технологического процесса, передается от нижнего уровня иерархии системы управления к верхнему. За расчет добытого объема газа отвечают расходомеры, которые измеряют поступающий в прибор газ равными по объему дозами, которые затем суммируются. Газ перед этим нагревается до определенной (стандартной) температуры. Масса газа при этом не измеряется. Поэтому если повлиять на прибор, ответственный за нагревание добытого газа перед подачей в расходомер, изменив температуру нагревания на некоторое количество градусов, то через расходомер можно пропустить бо́льший объем газа. Разницу между расчетными объемами газа, добытого при рабочей и измененной температурах, можно скрыто похитить.

Для реализации такого типа нарушения ИБ необходимо повлиять на показания системы, то есть сделать так, чтобы вместо заданных в систему попадали ложные показания, в которых заинтересован злоумышленник. Такого результата можно добиться, в частности, следующими способами: перепрограммированием ПЛК, ответственного за передачу информации о нагревании; при помощи вредоносного ПО попытаться исказить данные на АРМ, которое передает их для учета в SCADA-систему; использовать другие способы. Пример организации атак класса «хищение» представлен на рисунке 5.

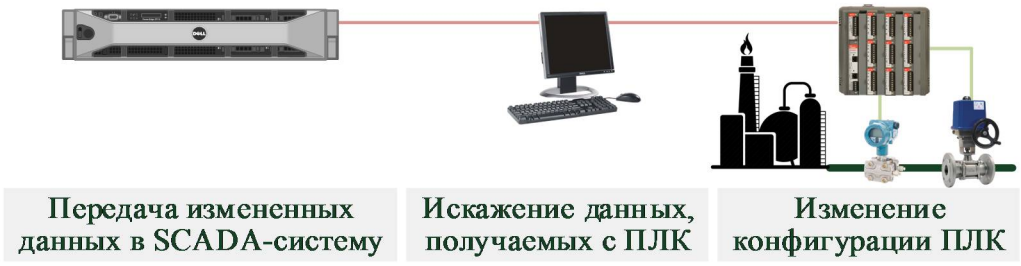


Рисунок 5 – Класс атак – хищение

Целевая кибератака. Целевые кибератаки применительно к АСУ ТП условно можно разделить на два вида:

- несанкционированное получение информации;
- нарушение технологического процесса.

Несанкционированное получение информации. Такой вид атак направлен на использование АСУ ТП с целью повлиять на производственный процесс предприятия. Это влияние может быть либо промышленным шпионажем (чтобы разведать данные ограниченного доступа), либо саботажем, направленным на дезорганизацию или прекращение производственного процесса. Учтем следующее: каждое ГДП добывает ресурсы на выделенных лицензионных участках, а организаций, обладающих лицензией на добычу газа, в стране ограниченное количество, и их деятельность во многом контролируется государством. Поэтому конкурентная разведка между такими компаниями в России обычно нецелесообразна, но указанные сведения могут представлять интерес для иностранных организаций, в том числе конкурирующих с российскими на зарубежных рынках сбыта газа или продуктов его переработки.

Информацией ограниченного доступа является любая информация, которой может воспользоваться злоумышленник для нанесения ущерба предприятию. Такой информацией могут являться конфигурации ПЛК, данные с пульта управления оператора, архивные сведения SCADA-системы и другие, по которым можно восстановить технологический процесс. Полученную информацию можно использовать для оказания влияния на производство и организацию других видов атак, в некоторых случаях – для нанесения репутационных ущербов предприятиям.

Источники информации ограниченного доступа представлены на рисунке 6.

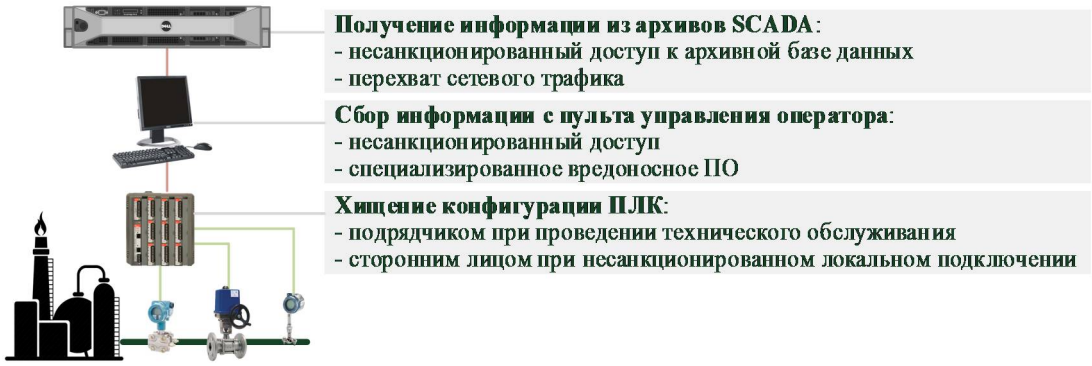


Рисунок 6 – Направленная атака с целью получения информации

Нарушение технологического процесса. Разрушить (нарушить) техпроцесс на ГДП можно несколькими способами. Одним из них является доведение производственного процесса до аварийного состояния путем, например, перепрограммирования ПЛК или АРМ, отвечающий за давление газа в трубах, отходящих от газодобывающих скважин. Учитывая, что газодобывающее предприятие является опасным объектом, на нем, как правило, предусмотрены аварийные ситуации, и реализуемые процессы контролируются нормами промышленной безопасности. Поэтому в случае выхода каких-либо показателей за допустимые пределы независимая система (по сравнению с АСУ ТП) отключает эти объекты.

Менее очевидной атакой на техпроцесс будет являться атака, имеющая целью оказание влияния на конечный добываемый продукт. Как и в примере с хищением, можно, например, повлиять на логику работы устройств АСУ ТП, подменив алгоритмы (в частности изменить принцип работы механизмов, отвечающих за отделение газа от конденсата). Таким образом, в результате добываемый газ будет иметь другую консистенцию и соответственно другое качество. Это может в дальнейшем сказаться на репутации компании и привести к серьезному экономическому ущербу для нее. Возможные сценарии целевых кибератак, направленных на нарушение технологического процесса, представлены на рисунке 7.

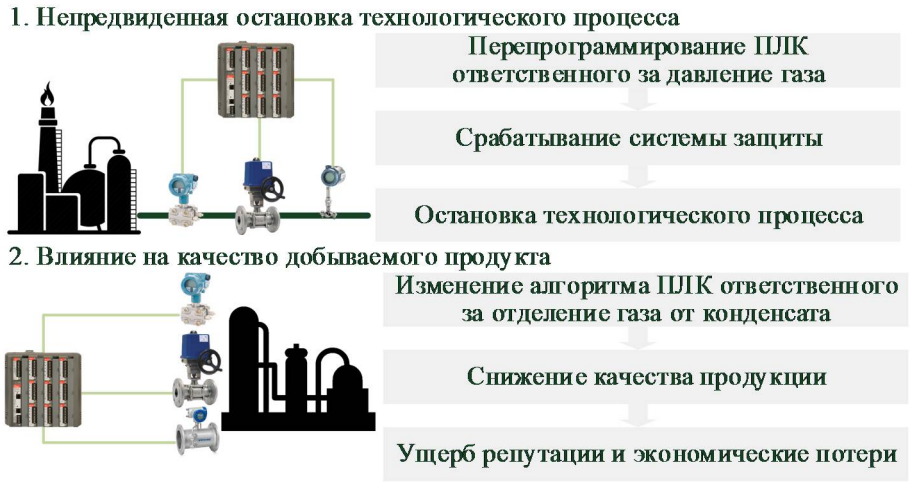


Рисунок 7 – Сценарии целевых кибератак, направленных на нарушение технологического процесса ГДП

Стадии атаки на АСУ ТП. Суммируя вышесказанное, можно прийти к выводу, что любая атака на АСУ ТП, связанная с технологическим процессом, будет состоять из трех основных стадий, которые начинаются на верхнем уровне АСУ ТП и заканчивается на нижнем.

Первая стадия – это IT-атака через человеко-машинный интерфейс АСУ ТП или подключение к смежным системам – основным звеньям АСУ ТП. Они обычно используют популярные вне промышленных систем IT-решения, содержащие общеизвестные уязвимости и, как следствие, подверженные традиционным атакам, в рамках которых злоумышленник проникает в защищаемый периметр АСУ ТП с целью дальнейших действий.

Вторая стадия – это следующий этап атаки, где уязвимыми объектами являются технологические компоненты системы, например, логика работы SCADA-системы или алгоритмы ПЛК. При этом целью является создание сбоев в работе АСУ ТП, манипуляции технологическими процессами и пр.

Третья стадия – атака на технологические объекты управления, которые управляются ПЛК. На этой стадии целью является нанесение максимального ущерба. В качестве примера можно привести поведение известного компьютерного червя Stuxnet, который скрытно увеличивал скорости вращения центрифуг в системах обогащения 235-м изотопом шестифтористого урана.

Червь поражал непосредственно ПЛК, заставляя центрифуги работать в предельно допустимом режиме. Это приводило к повышенному износу оборудования, но не к мгновенному выходу их из строя. После выхода из строя нескольких центрифуг подряд логично было бы провести внеочередное техническое обслуживание, дополнительную наладку и найти отклонение. Поэтому преждевременный износ оборудования был растянут по времени, чтобы центрифуги не начали выходить из строя почти одновременно и тем самым разоблачить действия зловредного ПО. При этом Stuxnet добивался того, чтобы центрифуги выходили из строя быстрее, чем их успевали бы пополнить (заменить). Для организации атаки на таком технологическом уровне необходимо обладать информацией о том, как устроен технологический процесс, которым управляют атакуемые АСУ ТП.

Считается, что область ИБ заканчивается там, где начинается технологический объект управления и происходит переход к промышленной безопасности. Ее задачей является в первую очередь безопасное функционирование системы, а именно отсутствие человеческих жертв и минимальный экологический ущерб. Задачей ИБ в свою очередь является нейтрализация злоумышленника на второй стадии. Этапы (стадии) атаки на АСУ ТП представлены на рисунке 8.

Рисунок 8 – Стадии атаки на АСУ ТП

Актуальные классы решений, направленных на обеспечение ИБ АСУ ТП ГДП. Большинство решений на рынке для обеспечения ИБ представляют собой сочетания программных и аппаратных «инструментов»; для реализации своего функционала требуют интеграции в промышленную сеть. Учитывая, что АСУ ТП ГДП представляет собой непрерывный процесс по добыче природного газа, внедрение подобных средств обеспечения ИБ в системах, в которых изначально не было предусмотрено и протестировано их использование, может частично или полностью неблагоприятно повлиять на весь технологический процесс [7]. Возможные проблемы могут быть вызваны как несовместимостью оборудования или ПО, так и встроенным функционалом блокирования дополнительных программно-аппаратных средств. С учетом того, что газовое предприятие является опасным промышленным объектом, подобное воздействие может быть причиной отказа оборудования или даже аварии. Поэтому при выборе решений для защиты системы необходимо руководствоваться в первую очередь минимальным вмешательством в производственные процессы.

Из предлагаемых на рынке классов решений, оказывающих минимальное воздействие на систему и повышающих уровень ее ИБ, можно выделить следующие «классы» [25]:

- средства межсетевого экранирования;
- системы обеспечения одностороннего межсетевого взаимодействия;
- системы обнаружения вторжений;
- дублирование и перенаправление технологического трафика;
- корреляция инцидентов и мониторинг событий ИБ;
- сканеры уязвимостей;
- средства моделирования угроз.

Далее эти классы решений рассматриваются более подробно.

Межсетевой экран (МЭ) – это система сетевой безопасности, которая отслеживает и контролирует входящий и исходящий сетевой трафик на основе заранее определенных правил безопасности.

МЭ обычно подразделяются на сетевые и хостовые. Сетевые брандмауэры расположены на компьютерах-шлюзах локальных сетей, глобальных сетей и интрасетей. Они представляют собой либо программные решения, работающие на основе аппаратного обеспечения общего назначения, либо отдельные устройства со встроенной ОС. МЭ на основе хоста расположены на самом сетевом узле и контролируют входящий и исходящий сетевой трафик этих устройств.

У каждого типа МЭ свои преимущества и недостатки. Однако в промышленных сетях применение чаще находит сетевой тип МЭ. Его используют для установки барьера между доверенной внутренней сетью и «ненадежной» внешней сетью. В случае АСУ ТП ГДП это соответствует следующему: между промышленной сетью и корпоративной.

Иногда МЭ может применяться и внутри промышленной сети между верхним и средним уровнем для контроля сетевого трафика. В этом случае правила доступа настраиваются таким образом, что в список открытых портов входят необходимые промышленные протоколы. Например, открывается доступ по порту TCP 502 (Modbus TCP).

Одной из разновидностей МЭ являются «промышленные полевые МЭ» – они используются на уровне контроллеров. Основными вендорами, поставляющими подобный тип оборудования, являются зарубежные компании, однако ведутся и отечественные разработки в данном направлении [2]. На рисунке 9 представлен пример использования промышленных МЭ.

Основным отличием промышленных полевых МЭ является контроль сессии промышленных протоколов на прикладном уровне, а не только на сетевом. Таким образом, промышленные полевые МЭ могут проводить полноценную инспекцию промышленных протоколов на уровне приложений, позволяя тем самым более гибко настраивать допустимый в промышленной сети трафик.

При защите промышленной сети между уровнями АСУ ТП также важными являются технические характеристики, такие как требования к вибрационным нагрузкам, рабочей температуре, влагоустойчивости. Исходя из данных параметров, можно определить, насколько конкретное устройство будет удовлетворять эксплуатационным требованиям к сетевому оборудованию на конкретном объекте.

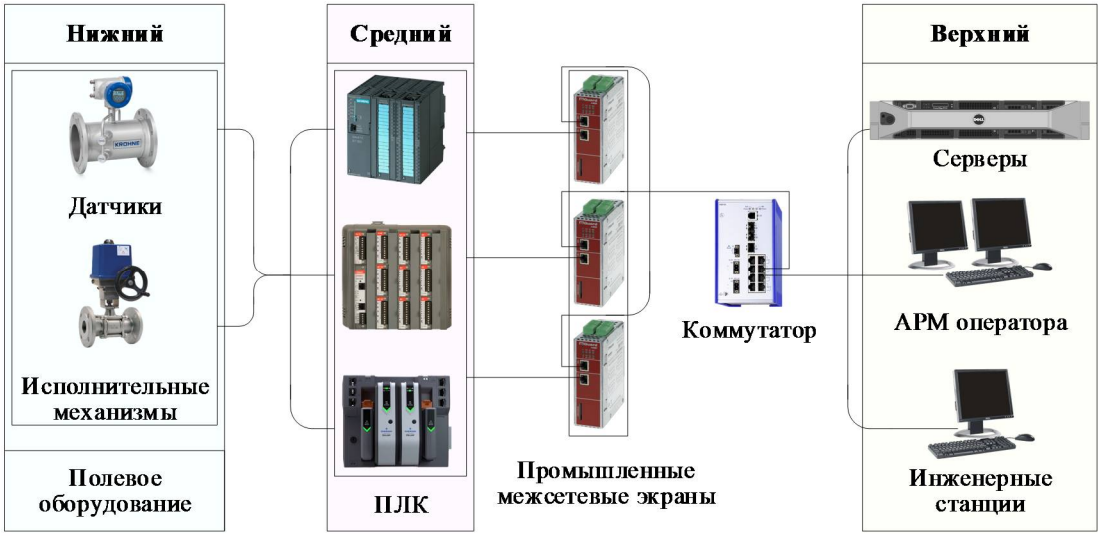


Рисунок 9 – Применение промышленного МЭ

Системы одностороннего межсетевого взаимодействия (также известные как однонаправленные шлюзы и диоды данных) – это устройства связи, которые обеспечивают безопасную одностороннюю передачу данных между сегментированными сетями. Интеллектуальная конструкция таких систем поддерживает физическое и электрическое разделение сетей источника и назначения. При этом устанавливается немаршрутизируемый, полностью закрытый, односторонний протокол передачи данных между сетями. Обеспечение безопасности всех потоков данных в сети с помощью систем одностороннего межсетевого взаимодействия делает невозможной передачу небезопасных или враждебных вредоносных программ, а также удаленный доступ к промышленным системам [17].

Таким образом, применение технологий односторонних шлюзов в промышленных сетях ГДП позволяет безопасно передавать информацию только в одном направлении, от защищенных областей (АСУ ТП) к менее защищенным системам (корпоративный сегмент сети), исключая возможность проникнуть в промышленную сеть извне. Подобное решение в отличие от более популярных (OPC- (Open Platform Communications), MES- (Manufacturing Execution System) серверов) намного эффективнее защищает от попыток несанкционированного доступа в сеть АСУ ТП, так как злоумышленник на физическом уровне не имеет доступа из корпоративного сегмента в промышленный.

Для полноценной работы «диода данных» ему необходимы прокси-серверы: внутренний (находится в промышленном сегменте сети) и внешний (находится в корпоративном сегменте сети). Взаимодействие между прокси-серверами происходит в одном направлении, например, от внешнего к внутреннему. В обратном направлении прокси-серверы не могут взаимодействовать в силу использования «диода данных». В нем на аппаратном уровне исключен интерфейс в отношении приема информации от внутреннего прокси-сервера. Схема устройства «диода данных» представлена на рисунке 10.

Существует множество вариантов использования систем одностороннего межсетевого взаимодействия в АСУ ТП ГДП:

- отправка данных через OPC Server о добываемых ресурсах в сегмент корпоративной сети для мониторинга и анализа информации;
- обеспечение взаимодействия компонентов иерархии WSUS (Windows Server Update Services) сегментов корпоративной сети и АСУ ТП;
- пересылка журналов аудита в формате syslog для SIEM-систем (Security Information and Event Management), расположенных вне сегмента АСУ ТП;
- удаленное обслуживание оборудования АСУ ТП с привлечением квалифицированной сервисной поддержки, исключающей утечки информации.

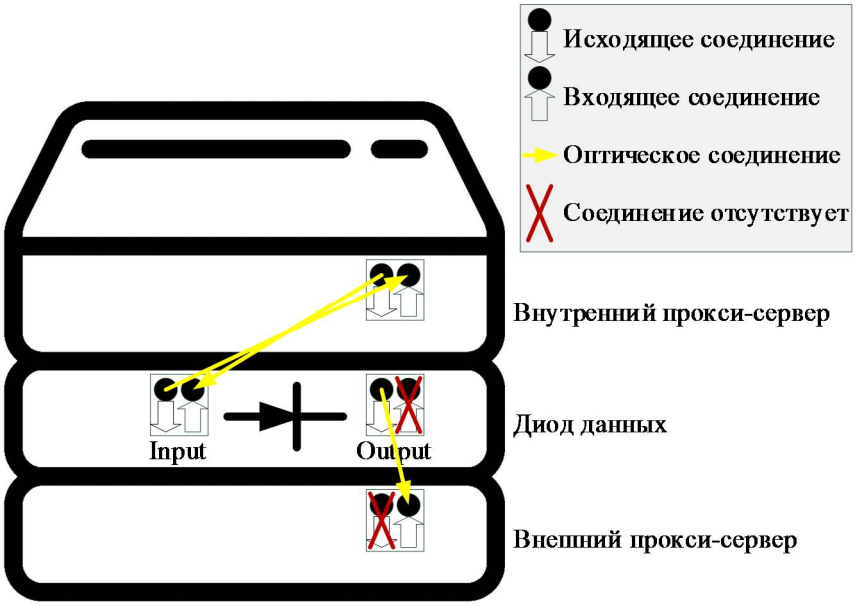


Рисунок 10 – Схема устройства диода данных [8]

На рисунке 11 представлен один из примеров использования «диода данных» в промышленной сети.

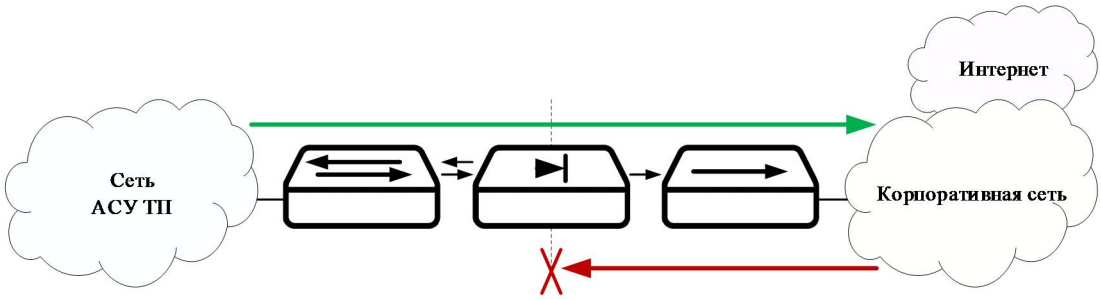


Рисунок 11 – Пример использования «диода данных» в промышленной сети

Система обнаружения вторжений (СОВ) – это аппаратное или программное решение, которое отслеживает сеть или системы на предмет вредоносных действий или нарушений политики безопасности. О любых злонамеренных действиях или нарушениях обычно либо сообщается администратору, либо информация об этих действиях собирается централизованно с использованием системы защиты информации и управления событиями (SIEM) [18].

Основное отличие СОВ от МЭ заключается в том, что МЭ ограничивает доступ между сетями, чтобы предотвратить вторжение, и не сигнализирует о нападении внутри сети. СОВ в свою очередь описывает предполагаемое вторжение после того, как оно произошло, и сигнализирует об опасности. Также СОВ отслеживает атаки, исходящие из ОС. Указанные возможности достигаются путем изучения сетевых взаимодействий, выявления эвристики и сигнатур распространенных компьютерных атак; принятия мер по предупреждению операторов АСУ ТП, специалистов по ИБ.

Типы СОВ варьируются, и они применяются, начиная от отдельных компьютеров и до крупных сетей. Наиболее распространенными классификациями СОВ являются сетевые системы обнаружения вторжений (NIDS) и хост-системы обнаружения вторжений (HIDS). Система, которая отслеживает важные файлы операционной системы, является примером HIDS, а система, которая анализирует входящий сетевой трафик, является примером NIDS. Также можно классифицировать СОВ с помощью подхода к обнаружению. Наиболее известные варианты – это сигнатурное обнаружение (распознавание опасных сигнатур, таких как вредоносные программы или атаки) и обнаружение на основе аномалий (обнаружение отклонений от модели допустимого трафика, которая часто опирается на машинное обучение).

Расширенный вариант СОВ со способностью реагирования на обнаруженные вторжения называется системой предотвращения вторжений. В промышленных сетях такое средство защиты не рекомендуется использовать в связи с потенциальной возможностью блокировки технологических процессов в случае обнаружения аномальной и вредоносной сетевой активности, что может существенно повлиять на всю промышленную сеть в целом. Поэтому использование СОВ с отсутствием возможности реагировать на обнаруженные вторжения является более приемлемым вариантом.

Дублирование и перенаправление сетевых пакетов (зеркалирование). Как правило, зеркалирование портов используется на сетевом коммутаторе для отправки копий всех или отдельно взятых VLAN входящих и/или исходящих сетевых пакетов, получаемых на одном или нескольких портах, на отдельный интерфейс для мониторинга сетевого трафика [19]. С точки зрения безопасности наиболее эффективно данный метод может использоваться совместно с предыдущим средством защиты – СОВ. Данный способ наиболее приемлемый для реализации при использовании в промышленных сетях СОВ, так как это гарантирует, что при анализе трафика отсутствуют угрозы для работы промышленной сети.

Еще одним полезным применением зеркалирования портов является анализ и отладка полученной информации или диагностики ошибок в сети. Это помогает системным администраторам внимательно следить за производительностью сети и оповещать их при возникновении проблем.

Корреляция инцидентов и мониторинг событий ИБ. В области компьютерной безопасности программные продукты и услуги по *защите информации и управлению событиями* (SIEM) объединяют управление информационной безопасностью (SIM) и управление событиями безопасности (SEM). Они обеспечивают в реальном времени анализ предупреждений безопасности, генерируемых приложениями и сетевым оборудованием.

SIEM может представлять из себя как программное или аппаратное решение, так и предоставляемую услугу [14]. Основное внимание уделяется мониторингу и управлению правами пользователей и служб, службами каталогов и другим изменениям конфигурации системы; а также реагированию на инциденты.

Система SIEM объединяет выходные данные из нескольких источников и использует методы фильтрации аварийных сигналов, чтобы отличить вредоносную активность от ложных аварийных сигналов. Это позволяет избавиться от необходимости следить за различными консолями средств защиты и вручную анализировать получаемую с них информацию о событиях, максимально автоматизировав и упростив этот процесс [12].

В случае, когда речь идет о технологическом сегменте предприятий, где необходим круглосуточный контроль исправности промышленных систем, помимо вышеуказанного функционала, данные решения могут стать одним из компонентов, используемых в «комплексном ситуационного центре». В его рамках формируется единая точка отслеживания как технических показателей систем и контроль процессов, так и мониторинг; управление информационной безопасностью предприятия.

Сканер уязвимостей – это компьютерная программа, предназначенная для оценки компьютеров, сетевой инфраструктуры или приложений на наличие известных уязвимостей. Они используются для выявления и обнаружения уязвимостей, возникающих из-за неправильной конфигурации или ошибок в программном коде сетевых устройств и программ, таких как МЭ, маршрутизатор, веб-сервер, сервер приложений и т.д. [23]. Современные сканеры уязвимостей позволяют выполнять сканирование как с аутентификацией, так и при ее отсутствии. Большинство сканеров уязвимостей имеют возможность формировать отчеты об уязвимостях, а также об установленном ПО, открытых портах, сертификатах и другую информацию об устройстве, которую можно запросить во время сканирования [16].

Использование сканеров уязвимостей в сетях АСУ ТП позволяет автоматизировать процесс поиска недочетов (недостатков) конфигурации используемого оборудования. Однако необходимо учитывать тот факт, что подобный класс решений также осуществляет нагрузку на промышленный траффик и оборудование. Вследствие этого может нарушаться непрерывный процесс управления технологическими системами.

Средства моделирования угроз. *Моделирование угроз* – это процесс, с помощью которого потенциальные угрозы, такие как структурные уязвимости, могут быть идентифицированы, перечислены и распределены по приоритетам на самом раннем этапе проектирования – с точки зрения гипотетического злоумышленника. Целью моделирования угроз является предоставление специалистам по защите информации систематического анализа профиля

вероятного злоумышленника, наиболее вероятных векторов атаки и активов организации, подверженных более вероятному нападению [20].

В отличие от сканеров уязвимостей средства моделирования угроз не нуждаются во взаимодействии с устройствами для анализа текущих уязвимостей. Поэтому в средствах моделирования угроз исключены такие недостатки сканеров уязвимостей, как влияние на промышленный трафик. Тем самым данный класс решений позволяет безопасно определить уязвимости оборудования АСУ ТП, однако в отличие от сканеров уязвимостей этап исследования инфраструктуры происходит не в автоматическом режиме. Также при помощи данного типа средств можно проводить анализ и осуществлять управление рисками использования АСУ ТП [10].

Как правило, процессы моделирования угроз, связанные с ИТ, начинаются с создания визуального представления анализируемого приложения или инфраструктуры сети. Они разбиваются на отдельные элементы, чтобы провести максимально подробный анализ всей системы в целом. После завершения анализа визуальное представление используется для перечисления потенциальных угроз. Дальнейший анализ модели в отношении рисков, связанных с выявленными угрозами, расстановкой приоритетов угроз и перечислением соответствующих «смягчающих угрозы» мер управления, зависит от методологической основы используемого процесса построения модели угроз [20]. При использовании средств моделирования угроз для управления рисками вместо угроз можно рассматривать также неблагоприятные события [4].

Моделирование угроз желательно выполнять на ранних этапах цикла проектирования АСУ ТП. При этом потенциальные проблемы могут быть выявлены на ранней стадии и устранены, что позволит избежать более дорогостоящих решений проблемы в будущем. Использование моделирования угроз для анализа требований безопасности может привести к использованию проактивных архитектурных решений, которые помогут уменьшить угрозы с самого начала эксплуатации системы.

Сравнение достоинств и недостатков рассмотренных классов решений. Для выбора наиболее безопасного решения, направленного на обеспечение ИБ АСУ ТП необходимо сформировать перечень критериев для сравнения рассмотренных классов. В качестве критериев будем использовать следующие характеристики:

- влияние на промышленный трафик;
- работа на всех уровнях АСУ ТП;
- изменение настроек используемого оборудования;
- использование рассматриваемого класса решений в проектируемом АСУ ТП.

На основании перечисленных критериев было проведено сравнение рассматриваемых классов решений в таблице 1.

Таблица 1 – Результаты сравнения актуальных классов решений обеспечения ИБ АСУ ТП

	Влияние на промышленный трафик	Работа на всех уровнях АСУ ТП	Изменение настроек используемого оборудования	Использование в проектируемом АСУ ТП
Средства МЭ	Влияет	Работает	Не изменяет	Неприменимо
Диод данных	Влияет	Работает	Не изменяет	Неприменимо
СОВ	Влияет	Работает	Изменяет	Неприменимо
Зеркалирование трафика	Не влияет	Работает	Изменяет	Неприменимо
SIEM-система	Влияет	Не работает	Изменяет	Неприменимо
Сканеры уязвимостей	Влияет	Не работает	Изменяет	Неприменимо
Средства моделирования угроз	Не влияет	Работает	Не изменяет	Применимо

В результате сравнения актуальных классов решения задач обеспечения ИБ АСУ ТП (табл. 1) можно видеть, что только два класса (зеркалирование трафика и средства моделирования угроз) при применении в АСУ ТП в случае их некорректной работы или получения доступа злоумышленником к данным средствам не повлияют на технологический процесс. Также, согласно приказу ФСТЭК России от 14.03.2014 № 31, установка и настройка средств защиты информации осуществляется в случаях, если такие средства необходимы для нейтрализации угроз безопасности информации, которые невозможно исключить настройкой АСУ ТП. Поэтому в первую очередь необходимо использовать встроенный функционал АСУ для повышения безопасности, в том числе для устранения уязвимостей текущей инфраструктуры.

Исходя из результатов, представленных в таблице 1, только три класса решений (МЭ, диод данных и средства моделирования угроз) не требуют никаких манипуляций с работающей системой: настройка сетевого оборудования и внедрение дополнительных программных или программно-аппаратных решений в промышленную сеть. Помимо этого, следует отметить, что только средства моделирования угроз позволяют эффективно спроектировать еще не существующую промышленную сеть, на ранних этапах устраняя потенциально возможные угрозы. Такой класс решений – наиболее безопасный инструмент для повышения уровня ИБ АСУ ТП ГДП [15].

К наиболее популярным и поддерживаемым на сегодняшний день относятся следующие решения в области моделирования угроз:

- ***Attack-Defense Tree Tool*** (ADTool) является компонентом обучающей платформы CybatiWorks, разработанным в университете Люксембурга в рамках проекта ATREES по созданию инструментария для составления дерева атак и планирования защитных мер [22]. ADTool позволяет пользователям моделировать и анализировать сценарии защиты от атак при помощи визуального создания «деревьев атак» и предполагаемых мер по их нейтрализации. Этот инструмент работает только с заранее подготовленными разработчиками моделями угроз, что очень сильно ограничивает возможности (объемы) его использование;
- ***Microsoft Threat Modeling Tool 2016*** – бесплатное решение для моделирования угроз от компании Microsoft, ориентированное на разработчиков ПО. Этот продукт допускает интегрирование в системы, используемые при отслеживании ошибок и других проблем в ПО. Несмотря на все преимущества этого инструмента, его применение для анализа угроз ИБ АСУ ТП ГДП нецелесообразно. Основная причина – в первую очередь это решение рассчитано на инвентаризацию угроз внутри или между приложениями. В то же время подавляющая часть программных продуктов, применяемых в АСУ ТП, является проприетарной, то есть к их исходным кодам имеют доступ только разработчики;
- ***OWASP Threat Dragon*** представляет собой веб-приложение для моделирования угроз в режиме онлайн. Предназначено для моделирования угроз на ранних этапах жизненного цикла разработки приложений. Главным недостатком этого решения (как и предыдущего) является направленность только на уязвимости и угрозы в приложениях. У данного программного средства отсутствует возможность моделирования угроз для сетевого оборудования или ОС – это делает его неприменимым при использовании в распределенной инфраструктуре;
- ***R-Vision Security GRC Platform*** – комплексный продукт от российской компании R-Vision. Одной из его частей является модуль по оценке рисков, поддерживающий функцию моделирования угроз. Данный инструмент помимо встроенных угроз поддерживает полную интеграцию с базой данных угроз (БДУ) ФСТЭК. Тем самым он обеспечивает возможности оценивания рисков ИБ в соответствии с текущими требованиями законодательства. Решение от R-Vision позволяет интегрировать его с различными системами защиты информации для дальнейшего моделирования угроз. Однако в случае отсутствия таких систем в промышленной сети в автоматическом режиме нельзя определить актуальные уязвимости в информационных активах организаций;
- ***ThreatModeler*** – автоматизированное решение от компании MyAppSecurity для моделирования угроз. Оно обеспечивает выявление, прогнозирование и определение угроз на протяжении всего жизненного цикла разработки приложений, а также возможность моделировать угрозы для облачных решений и IoT-устройств. В данном продукте отсутствует возможность дополнять базу угроз и уязвимостей. Поэтому моделирование угроз для нестандартного оборудования не представляется возможным. В свою очередь это ограничивает использование решения.

Учитывая специфические особенности обеспечения ИБ АСУ ТП [24], целесообразно определить основные критерии для сравнения рассмотренных средств моделирования угроз для ГДП:

- визуальное представление инфраструктуры промышленной сети;
- количественная оценка угроз и рисков;
- моделирование угроз для оборудования и ОС;
- пополняемость базы данных актуальными и собственными уязвимостями и угрозами.

На основании перечисленных критериев был проведен анализ на соответствие им у рассматриваемых средств моделирования угроз (табл. 2).

Таблица 2 – Результаты оценки соответствия средств моделирования угроз рассматриваемым критериям

	ADTool	Threat Modeling Tool 2016	Threat Dragon	Security GRC Platform	ThreatModeler
Визуальное представление сети	Да	Нет	Нет	Да	Нет
Количественная оценка угроз и рисков	Нет	Да	Нет	Нет	Да
Моделирование угроз для оборудования и ОС	Да	Нет	Нет	Да	Да
Пополняемость базы данных	Нет	Нет	Да	Да	Нет

Как следует из этой таблицы, многие из рассматриваемых решений ориентированы исключительно на уровень разработки ПО, и они не предназначены для корректного моделирования угроз промышленных сетей. Также многие из продуктов не позволяют моделировать угрозы с параметрами, которых не существуют в их базе. В связи с этим актуальной задачей является разработка средства моделирования угроз АСУ ТП для оценки рисков в ГДП.

Описание разработанного программного комплекса. Программный комплекс управления информационными рисками АСУ ТП ГДП «Risk Identification and Management Security Host-based Appliance» (R.I.M.S.H.A.) основан на методе количественной оценки рисков ИБ [21]. Он предназначен для идентификации существующих уязвимостей, моделирования угроз и оценки рисков ИБ в автоматизированных системах. Описываемый программный комплекс позволяет построить топологию АСУ ТП ГДП, связав все компоненты (АРМ-операторов и инженеров, сервера ввода-вывода информации, сетевое оборудование, ПЛК и др.) между собой, а также с газодобывающими установками. На основе построенной топологии рассчитывается потенциальный ущерб при реализации угроз для каждого из компонентов. На основе полученных данных оценивается риск для каждой из существующих в системе угроз. Программный комплекс также позволяет рассчитывать информационные риски для проектируемых промышленных систем [13].

В качестве используемой среды разработки ПО применялась Microsoft Visual Studio 2017. Используемый язык программирования – C#. В качестве базы данных использовалась SQLite.

На рисунке 12 представлен интерфейс главного окна программного комплекса R.I.M.S.H.A. с произвольно заданной топологией АСУ ТП.

Охарактеризуем назначение панелей.

«Панель для проектирования топологии» (область 1 на рис. 12) предназначена для построения топологии АСУ ТП путем перемещения иконок оборудования из панели «Список оборудования» (область 4 на рис. 12) на рабочее поле.

Панель «Тип оборудования» (область 3 на рис. 12) отображает список объектов множества компонентов. При выборе одного из элементов панели меняется список панели «Вид оборудования», находящейся в той же области. Панель «Вид оборудования» содержит различные виды определенного компонента. Например, у сетевых устройств такими «видами» могут являться маршрутизаторы, коммутаторы, межсетевые экраны и т.д.

На панели «Список оборудования» (область 4 на рис. 12) находится оборудование, при помощи которого создается проект топологии АСУ ТП газодобывающего предприятия.

В зависимости от выделенного объекта в панели «Свойства» (область 2 на рис. 12) отображаются его характеристики.

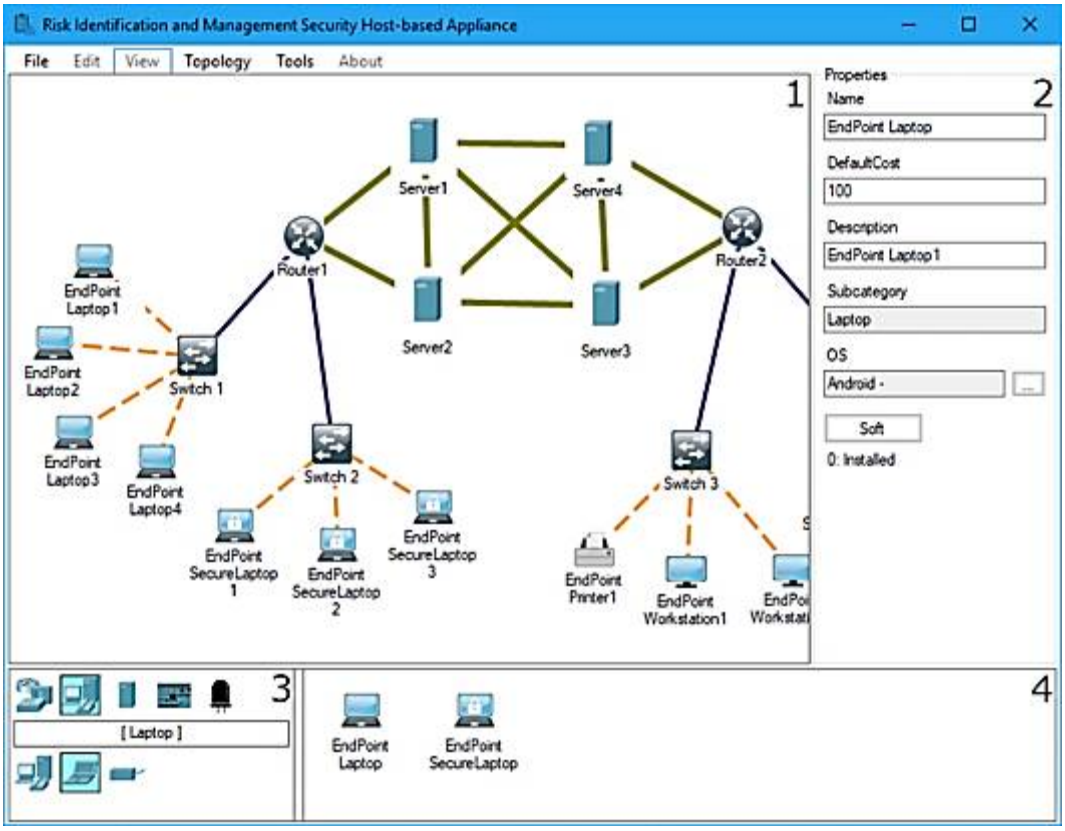


Рисунок 12 – Пример интерфейса главного окна программного комплекса

Источником выбора уязвимостей и угроз является база данных угроз ФСТЭК России. На рисунке 13 представлен интерфейс окна с отображением актуальных уязвимостей для указанной топологии.

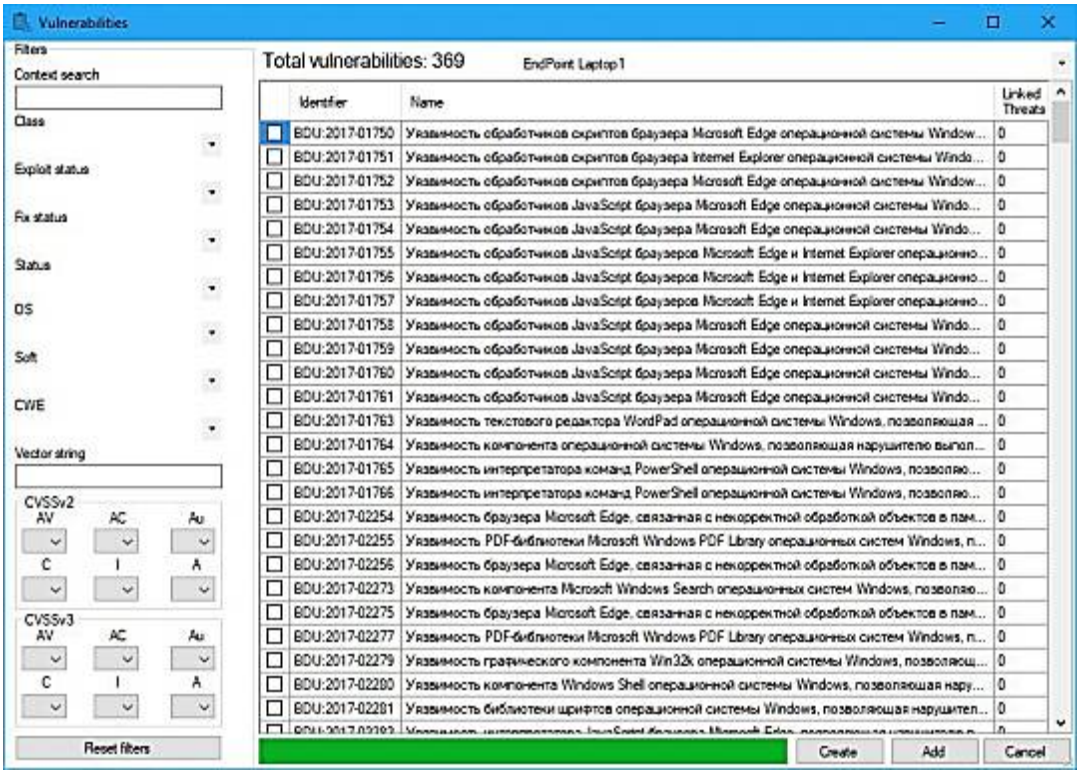


Рисунок 13 – Пример интерфейса окна с актуальными уязвимостями

Из выявленных уязвимостей при помощи «чекбоксов» можно создать выборку, которую можно либо добавить к существующей угрозе, либо создать новую. Также можно применять фильтры для поиска определенных уязвимостей.

На рисунке 14 представлен интерфейс окна программного комплекса с примером создания новой угрозы.

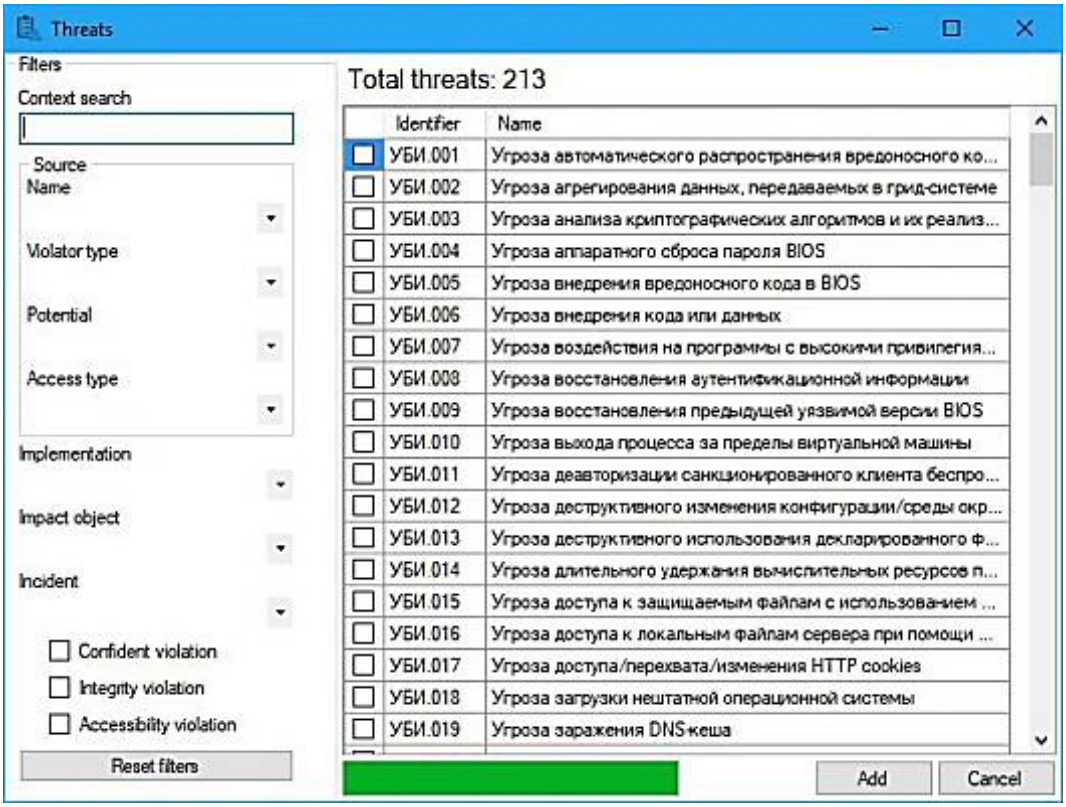


Рисунок 14 – Интерфейс окна с созданием новой угрозы

Программный комплекс R.I.M.S.H.A. автоматизирует процесс моделирования угроз и оценки рисков и позволяет делать следующее:

- спроектировать топологию АСУ ТП ГДП;
- рассчитать оценки угроз, ущерба и риска для каждого компонента;
- вести учет текущих уязвимостей, угроз и рисков для конкретной АСУ ТП.

Помимо этого, отличительной особенностью описываемого программного комплекса по сравнению с аналогами является возможность добавлять собственные уязвимости при помощи параметров CVSS с последующим объединением их в угрозы и автоматической оценкой риска. Таким образом, использование различных комбинаций произвольных уязвимостей позволяет подбирать наиболее эффективные стратегии защиты для АСУ ТП ГДП, не влияя на технологический процесс.

Заключение. В данной работе формально описан процесс работы типовых АСУ ТП и иерархическая структура ГДП. Рассмотрены основные типы нарушений ИБ в АСУ ТП и приведены примерные сценарии подобных нарушений. Выделены стадии атаки на АСУ ТП на основе рассматриваемых типов нарушений.

Проанализированы достоинства и недостатки актуальных классов решений для задач обеспечения ИБ АСУ ТП ГДП. Исходя из результатов сравнения, «средства моделирования угроз» были определены как наиболее эффективные и безопасные с точки зрения возможностей потенциальных воздействий на технологический процесс.

Учитывая, что из предлагаемых на рынке наиболее популярных решений ни одно в полной мере не походит для моделирования угроз АСУ ТП, авторы статьи использовали разработанный раннее метод моделирования угроз и оценки рисков [21] для создания собственного программного комплекса управления информационными рисками АСУ ТП ГДП.

Предложенный (разработанный) программный комплекс позволяет проводить анализ защищенности АСУ ТП ГДП с целью дальнейшего устранения диагностированных (выявленных) уязвимостей. Также комплекс предоставляет возможность смоделировать потенциальные уязвимости еще до начала внедрения какого-либо оборудования или ПО на предприятиях.

Библиографический список

1. Аникин И. В. Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками / И. В. Аникин, Л. Ю. Емалетдинова, А. П. Кирпичников // Вестник технологического университета. – 2015. – Т. 18, № 7. – С. 247–250

2. Аннушкин С. Л. О достижениях, сложностях и перспективах импортозамещения компонентной базы для отечественных промышленных автоматизированных систем управления (АСУ) / С. Л. Аннушкин // Информационные ресурсы России. – 2015. – № 6. – С. 15–19.

3. Блинков Ю. В. Основы автоматизации управления процессами и объектами : учебное пособие / Ю. В. Блинков. – Пенза : ПГУАС, 2009. – 172 с.

4. Брумштейн Ю. М. Анализ некоторых моделей группового управления рисками / Ю. М. Брумштейн, О. Н. Выборнова // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 4. – С. 64–72.

5. Дабагов А. Р. О проблемах безопасности в контексте открытой системной архитектуры / А. Р. Дабагов, С. А. Соколов // Радиолокация и радиосвязь : III Всероссийская конференция. – 2009. – С. 696–702.

6. Домуховский Н. Архитектура и основные компоненты АСУ ТП с точки зрения информационной безопасности. – Режим доступа: https://www.ussc.ru/events/zapisi-vebinarov/seriya-vebinarov-ib-asu-tp-non-stop/seriya-1-arkhitektura-i-osnovnye-komponenty-asu-tp-s-tochki-zreniya-informatsionnoy-bezopasnosti/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.08.2019).

7. Захаров А. А. Анализ информационной безопасности автоматизированных систем управления техническими процессами газодобывающего предприятия / А. А. Захаров, А. С. Римша, А. М. Харченко, И. Р. Зулькарнеев // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 3 (25). – С. 24–33.

8. Мальнев А. Защита АСУ ТП: от теории к практике. – Режим доступа: http://itsec.ru/articles2/Oborandteh/zaschita-asu-tp-ot-teorii-k-praktike, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.08.2019).

9. Римша А. С. Об одном подходе к формированию перечня мер по защите информации в беспроводных сенсорных сетях газодобывающего предприятия / А. С. Римша, А. Н. Югансон, К. С. Римша // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 2 (28). – С. 60–70.

10. Учаев Д. Ю. Анализ и управление рисками, связанными с информационным обеспечением человеко-машинных АСУ технологическими процессами в реальном времени / Д. Ю. Учаев, Ю. М. Брумштейн, И. М. Ажмухадедов, О. М. Князева, И. А. Дюдиков // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2. – С. 82–97.

11. Финогеев А. Г. Анализ и классификация атак через беспроводные сенсорные сети в SCADA системах / А. Г. Финогеев, И. С. Нефедова, Е. А. Финогеев, В. Т. Куанг, П. В. Ботвинкин // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 1. – С. 12–23.

12. Aguirre I. Improving the automation of security information management: A collaborative approach / I. Aguirre, S. Alonso // IEEE Security & Privacy. – 2011. – № 10 (1). – P. 55–59.

13. Colombo A. W. Towards the next generation of industrial cyber-physical systems / A. W. Colombo, K. Stamatis, B. Thomas // Industrial cloud-based cyber-physical systems. – Springer, Cham., 2014. – P. 1–22.

14. Coppolino L. Enhancing SIEM technology to protect critical infrastructures / L. Coppolino, S. D'Antonio, V. Formicola, L. Romano // Critical Information Infrastructures Security. – Berlin : Springer, 2013. – P. 10–21.

15. Myagmar S. Threat modeling as a basis for security requirements / S. Myagmar, A. J. Lee, W. Yurcik // Symposium on requirements engineering for information security (SREIS). – 2005. – P. 1–8.

16. Nilsson J. Vulnerability scanners / J. Nilsson, V. Virta // Master of Science Thesis at Department of Computer and Systems Sciences, Royal Institute of Technology. – Kista, Sweden, 2006. – P. 1–70.

17. Okhravi H. Data Diodes in Support of Trustworthy Cyber Infrastructure and Net-Centric Cyber Decision Support / H. Okhravi, F.T. Sheldon, J. Haines // Optimization and Security Challenges in Smart Power Grids. – 2013. – P. 203–216.

18. Oman P. Intrusion detection and event monitoring in SCADA networks / P. Oman, M. Phillips // International Conference on Critical Infrastructure Protection. – Boston : Springer, 2007. – P. 161–173.

19. Parry J. A network forensics tool for precise data packet capture and replay in cyber-physical systems / J. Parry, D. Hunter, K. Radke, C. Fidge // Proceedings of the Australasian Computer Science Week Multiconference. – 2016. – № 22. – P. 1–10.

20. Paté-Cornell M. E. Cyber Risk management for critical infrastructure: a risk analysis model and three case studies / M. E. Paté-Cornell, M. Kuypers, M. Smith, P. Keller // Risk Analysis. – 2017. – Vol. 38, № 2. – P. 226–241.

21. Rimsha A. S. Method for Risk Assessment of Industrial Networks' Information Security of Gas Producing Enterprise / A. S. Rimsha, A. A. Zakharov // 2018 Global Smart Industry Conference (GloSIC). – Chelyabinsk, 2018. – P. 1–5.

22. Saini V. Threat modeling using attack trees / V. Saini, Q. Duan, V. Paruchuri // Journal of Computing Sciences in Colleges. – 2008. – Vol. 23, № 4. – P. 124–131.

23. Samtani S. Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques / S. Samtani, S. Yu, H. Zhu, M. Patton, H. Chen // IEEE Conference on Intelligence and Security Informatics (ISI). – 2016. – P. 25–30.

24. Yang Y. On lightweight security enforcement in cyber-physical systems / Y. Yang, J. Lu, K. K. R. Choo, J. K. Liu // Lightweight Cryptography for Security and Privacy. – Springer, Cham., 2015. – P. 97–112.

25. Zegzhda D. P. Approach to APCS protection from cyber threats / D. P. Zegzhda, T. V. Stepanova // Automatic Control and Computer Sciences. – 2015. – № 49 (8). – P. 659–664.

References

1. Anikin I. V., Emaletdinova L.Yu., Kirpichnikov A. P. Obespechenie informatsionnoy bezopasnosti korporativnyh informatsionnyh setey cherez otsenku i upravlenie riskami [Ensuring information security of corporate information networks through risk assessment and management]. *Vestnik tekhnologicheskogo universiteta* [Issues of University of Technology], 2015, vol. 18, no. 7, pp. 247–250.

2. Annushkin S. L. O dostizheniyakh, slozhnostyakh i perspektivakh importozameshcheniya komponentnoy bazy dlya otechestvennykh promyshlennykh avtomatizirovannykh sistem upravleniya (ASU) [About achievements, difficulties and perspectives of import substitution in the field of the component base for Russian industrial automatic control systems (ACS)]. *Informatsionnye resursy Rossii* [Information resources of Russia], 2015, no. 6, pp. 15–19.

3. Blinkov Yu. V. *Osnovy avtomatizatsii upravleniya protsessami i obektami* [Fundamentals of automation of process and object management]. Penza, 2009, 172 p.

4. Brumshteyn Yu. M., Vybornova O. N. Analiz nekotorykh modeley gruppovogo upravleniya riskami [Analysis of some models for group risk management]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii [*Caspian Journal: Control and High Technologies], 2015, no. 4, pp. 64–72.

5. Dabagov A. R., Sokolov S. A. O problemakh bezopasnosti v kontekste otkrytoy sistemnoy arkhitektury [About security issues in the context of an open system architecture]. *Radiolokatsiya i radiosvyaz : III Vserossiyskaya konferentsiya* [Radiolocation and Radio Communication : The Third All-Russian Conference], 2009, pp. 696–702.

6. Domukhovskiy N. Arkhitektura i osnovnye komponenty ASU TP s tochki zreniya informatsionnoy bezopasnosti [Architecture and main components of industrial control system in terms of information security]. Available at: https://www.ussc.ru/events/zapisi-vebinarov/seriya-vebinarov-ib-asu-tp-non-stop/seriya-1-arkhitektura-i-osnovnye-komponenty-asu-tp- s-tochki-zreniya-informatsionnoy-bezopasnosti/ (accessed 26.08.2019).

7. Zakharov A. A., Rimsha A. S., Kharchenko A. M., Zulkarneev I. R. Analiz informatsionnoy bezopasnosti avtomatizirovannykh sistem upravleniya tekhnicheskimi protsessami gazodobyvayushchego predpriyatiya [Analysis of Information Security of Automated Control Systems for Technical Processes of a Gas Producing Enterprise]. *Vestnik UrFO. Bezopasnost v informatsionnoy sfere* [Bulletin of the Ural Federal District. Information Security], 2017, no. 3 (25). pp. 24–33.

8. Malnev A. Zashchita ASU TP: ot teorii k praktike [Protection of industrial control systems: from theory to practice]. Available at: http://itsec.ru/articles2/Oborandteh/zaschita-asu-tp-ot-teorii-k-praktike (accessed 26.08.2019).

9. Rimsha A. S., Yuganson A. N., Rimsha K. S. Ob odnom podkhode k formirovaniyu perechnya mer po zashchite informatsii v besprovodnykh sensornykh setyakh gazodobyvayushchego predpriyatiya [On One Approach to the Formation of a List of Measures to Protect Information in Wireless Sensor Networks of a Gas Producing Enterprise]. *Vestnik UrFO. Bezopasnost v informatsionnoy sfere* [Bulletin of the Ural Federal District. Information Security], 2018, no. 2 (28). pp. 60–70.

10. Uchaev D. Yu., Brumshteyn Yu. M., Azhmukhamedov I. M., Knyazeva O. M., Dyudikov I. A. Analiz i upravlenie riskami, svyazannymi s informatsionnym obespecheniem cheloveko-mashinnykh ASU tekhnologicheskimi protsessami v realnom vremeni [Analysis and management of risks, concerned with information support of human-machine automated control systems, operating in real time]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2016, no. 2, pp. 82–97.

11. Finogeev A. G., Nefedova I. S., Finogeev Y. A., Kuang V. T., Botvinkin P. V. Analiz i klassifikatsiya atak cherez besprovodnye sensornye seti v SCADA sistemakh [Analysis and classification of attacks via wireless sensor networks in SCADA systems]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 1, pp. 12–23.

12. Aguirre I., Alonso S. Improving the automation of security information management: A collaborative approach. *IEEE Security & Privacy*, 2011, no. 10 (1), pp. 55–59.

13. Colombo A.W., Stamatis K., Thomas B. Towards the next generation of industrial cyber-physical systems. *Industrial cloud-based cyber-physical systems*. Springer, Cham, 2014, pp. 1–22.

14. Coppolino L., D'Antonio S., Formicola V., Romano L. Enhancing SIEM technology to protect critical infrastructures. *Critical Information Infrastructures Security*. Berlin, Springer, 2013, pp. 10–21.

15. Myagmar S., Lee A. J., Yurcik W. Threat modeling as a basis for security requirements. *Symposium on requirements engineering for information security (SREIS)*, 2005, pp. 1–8.

16. Nilsson J., Virta V. Vulnerability scanners. *Master of Science Thesis at Department of Computer and Systems Sciences, Royal Institute of Technology*. Kista, Sweden, 2006, pp. 1–70.

17. Okhravi H., Sheldon F. T., Haines J. Data Diodes in Support of Trustworthy Cyber Infrastructure and Net-Centric Cyber Decision Support. *Optimization and Security Challenges in Smart Power Grids*, 2013, pp. 203–216.

18. Oman P., Phillips M. Intrusion detection and event monitoring in SCADA networks. *International Conference on Critical Infrastructure Protection*. Boston, Springer, 2007, pp. 161–173.

19. Parry J., Hunter D., Radke K., Fidge C. A network forensics tool for precise data packet capture and replay in cyber-physical systems. *Proceedings of the Australasian Computer Science Week Multiconference*, 2016, no. 22, pp. 1–10.

20. Paté-Cornell M. E., Kuypers M., Smith M., Keller P. Cyber Risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, 2017, vol. 38, no. 2, pp. 226–241.

21. Rimsha A. S., Zakharov A. A. Method for Risk Assessment of Industrial Networks' Information Security of Gas Producing Enterprise. *Global Smart Industry Conference (GloSIC)*. Chelyabinsk, 2018, pp. 1–5.

22. Saini V., Duan Q., Paruchuri V. Threat modeling using attack trees. *Journal of Computing Sciences in Colleges*, 2008, vol. 23, no 4. pp. 124–131.

23. Samtani S., Yu S., Zhu H., Patton M., Chen H. Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. *IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 25–30.

24. Yang Y., Lu J., Choo K. K. R., Liu J. K. On lightweight security enforcement in cyber-physical systems. Lightweight Cryptography for Security and Privacy, Springer, Cham, 2015, pp. 97–112.

25. Zegzhda D. P., Stepanova T. V. Approach to APCS protection from cyber threats. *Automatic Control and Computer Sciences*, 2015, no. 49 (8), pp. 659–664.

УДК 004.056.53

КОНЦЕПЦИЯ ЗАЩИТЫ ДАННЫХ В ОТКРЫТОЙ ЦИФРОВОЙ ПЛАТФОРМЕ МАССОВЫХ ПСИХОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ DigitalPsyTools.ru[1]

Статья поступила в редакцию 30.08.2019, в окончательном варианте – 02.09.2019.

Пушкин Павел Юрьевич, МИРЭА – Российский технологический университет, 119454, Российская Федерация, г. Москва, пр. Вернадского, 78,

кандидат технических наук, доцент кафедры «Управление и моделирование систем», e-mail: is-irk@mail.ru

Никульчев Евгений Витальевич, МИРЭА – Российский технологический университет, 119454, Российская Федерация, г. Москва, пр. Вернадского, 78,

доктор технических наук, профессор кафедры «Управление и моделирование систем», http://orcid.org/0000–0003–1254–9132, https://elibrary.ru/author_items.asp?authorid=396636, e-mail: nikulchev@mail.ru

Малых Сергей Борисович, Психологический институт Российской академии образования, 125009, Российская Федерация, г. Москва, ул. Моховая, 9, стр. 4,

академик РАО, доктор психологических наук, профессор, заведующий лабораторией возрастной психогенетики, https://elibrary.ru/author_items.asp?authorid=71885, e-mail: malykhsb@mail.ru

Обеспечение защиты прав и свобод граждан при обработке их персональных и обезличенных данных в цифровых платформах и информационных системах при организации и проведении массовых психологических исследований является важнейшей задачей организаторов проведения таких исследований. Проведение массовых психологических исследований имеет свои специфические особенности, которые определяются их целями и задачами. В статье сформирован концептуальный подход к проблеме защиты персональных и обезличенных данных при проведении массовых психологических исследований с использованием психологической платформы, разработаны основные положения определяющие политику оператора психологической платформы в отношении обработки персональных и обезличенных данных, определены совместные меры по обеспечению безопасности обрабатываемых данных для участвующих в организации и проведении психологических исследований сторон.

Ключевые слова: цифровая платформа, психологическая платформа, массовые психологические исследования, персональные данные, обезличенные данные, защита информации

[1] Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации, проект 25.13253.2018/12.1 «Разработка технологической концепции Дата-центра междисциплинарных исследований в образовании».