Integrated Approach to Cyber Risk Management:

Ensuring Operational Safety in Oil&Gas Sector

Интегрированный подход к управлению киберрисками:

обеспечение безопасности операционной деятельности в нефтегазовом секторе

Denis Lipov, Director, Head of Cyber Risk Management, Deloitte CIS
Anatoly Ostroglazov, Senior Manager, Deloitte CIS

Денис Липов, директор, руководитель направления по управлению кибер-рисками «Делойт», СНГ
Анатолий Остроглазов, старший менеджер «Делойт», СНГ

Today, the oil and gas sector is entering a new stage of development, which implies the rapid integration of robotic systems, digital innovations and Internet of Things (IoT) technology into the operating processes of enterprises.

Over the past 10 years, the interest of cybercriminals in industrial operations has been growing. This leads to the fact that all types of productive assets, including oil fields, oil pipelines and refineries, become vulnerable to cyberattacks, damaging both companies' production and safety. As a result, more and more companies are developing large-scale transformation programs to prevent new operational threats.

Industrial control system (ICS) is the basis for safety and functioning reliability of the most important infrastructural facilities. Over the past few years, the conventional boundaries between corporate ICSs and information systems have practically disappeared in the oil and gas sector. And this evolution goes on due to oil and gas companies' digitalization. As the connectivity between these types of systems is strengthened, cyberattacks will continue to grow in frequency and sophistication. Nevertheless, until now most companies can not cope with the task of preparing systems for cyberattacks.

Insufficient understanding of the importance of security measures within the enterprise leads to realization of cyber risks typical for corporate systems. For example, if companies use unprotected remote access to interact with the company's information resources, this allows cybercriminals to gain control over the systems managing production processes and cause production equipment reboot. In addition, incorrect testing of information systems before their deployment leads to their complete failure and, as a result, to production processes failures or shutdowns. There are many sources of cyberthreats, including company employees who are trying to organize a diversion in production, as well as competitors who want to damage the company's brand.

Regardless of whether there was a leak of data due to an oversight of the company itself or as a result of an attack by intruders, its consequences can be very serious: from data confidentiality compromise to systems failure or complete shutdown. And this may result in decrease in revenues, goodwill impairment, ecological catastrophe and loss of life in the worst case.

To improve the safety of operational processes, the oil and gas company must assess the maturity of the means to ensure control over the information security of production processes. Sufficient attention should be paid to the analysis of the connection between the risks associated with ICS crack, and

Сегодня нефтегазовый сектор выходит на новый этап развития, который подразумевает стремительную интеграцию роботизированных систем, цифровых инноваций и технологии Интернета вещей (IoT) в операционные процессы предприятий.

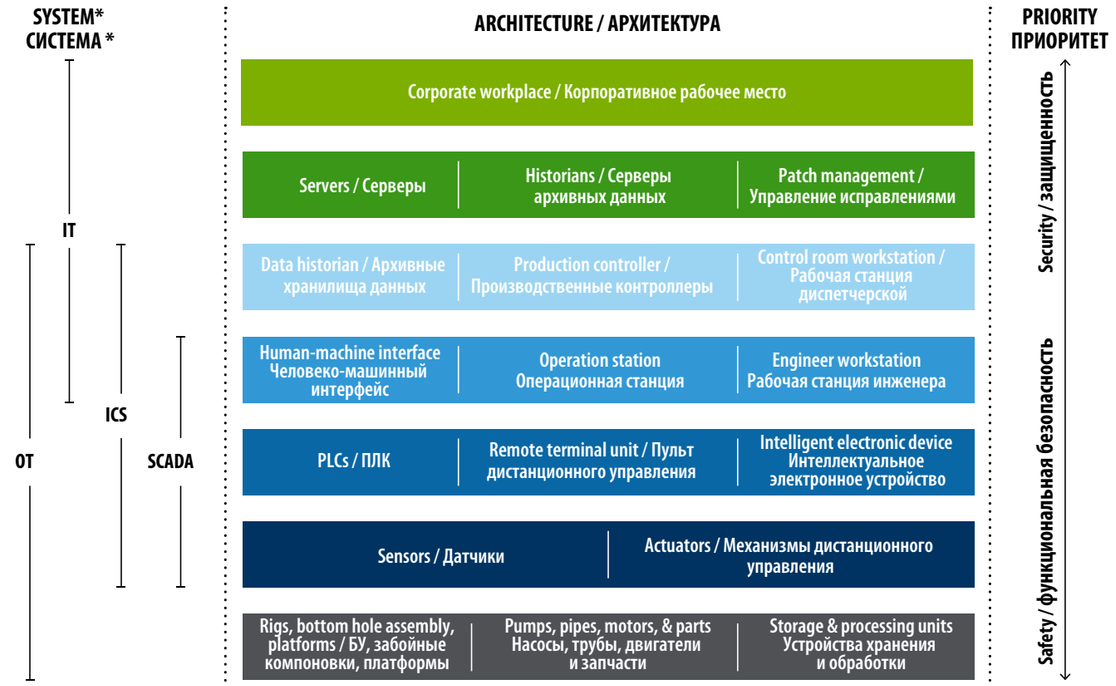
На протяжении последних 10 лет интерес киберпреступников к промышленным операциям растет. Это приводит к тому, что все виды производственных активов, включая нефтяные месторождения, нефтепроводы и нефтеперерабатывающие предприятия, становятся уязвимыми для кибератак, наносящих ущерб как производству, так и безопасности компаний. В результате все больше компаний ведет разработку масштабных трансформационных программ с целью предотвращения новых операционных угроз.

Основу безопасности и надежности функционирования наиболее важных объектов инфраструктуры составляют системы управления производственными процессами предприятий (ICS). За прошедшие несколько лет в нефтегазовом секторе практически стерлись привычные границы между корпоративными ICS-системами и информационными системами. Благодаря диджитализации нефтегазовых компаний эта эволюция продолжается. По мере того как взаимосвязь между указанными видами систем будет укрепляться, продолжат расти частотность и изощренность кибератак. Тем не менее, до сих пор большинство компаний не справляется с задачей подготовки систем к кибератакам.

Недостаточное понимание значения мер по обеспечению безопасности в рамках предприятия приводит к реализации киберрисков, присущих корпоративным системам. К примеру, если компании пользуются незащищенным удаленным доступом для взаимодействия с информационными ресурсами компании, это позволяет киберпреступникам получить контроль над системами, управляющими производственными процессами, и вызвать перегрузку производственного оборудования. Кроме того, некорректное проведение тестирования информационных систем перед развертыванием приводит к их полному отказу и, как следствие, к сбоям или остановке производственных процессов. Существует множество источников киберугроз, в том числе в лице сотрудников компании, стремящихся организовать диверсию на производстве, а также конкурентов, желающих нанести ущерб бренду компании.

Вне зависимости от того, произошла утечка данных по недосмотру самой компании или в результате атаки злоумышленников, ее последствия могут быть очень серьезными: от нарушения конфиденциальности данных до отказа или полной остановки работы систем. А это может повлечь за собой уменьшение объемов выручки, нанесение ущерба репутации

Figure 1. Typical IT/OT architecture and cyber concerns of an O&G company
Рисунок 1. Типичная архитектура ИТ / ОТ и кибер-проблемы компании O & G



CYBER CONCERNS

- Complex ecosystem: Joint operations take place across regions and employ multiple vendors with different security guidelines.
- Fragmented ownership: IT and OT were developed with distinct missions, thus cyber ownership and responsibility are fragmented across the organization.
- Latency concern: Firewalls could introduce unacceptable latency into time-critical ICS systems that face operational constraints.
- Inconsistent cyber standards: A mix of proprietary and off-the-shelf technologies complicates the problem.
- Irregular patching: Security patching of many systems is irregular and vendor specific as these systems are in remote, unmanned areas.
- Legacy concerns: Many systems have long life cycles (10+ years) that were not built for cybersecurity. Retrofitting or upgrading is costly and impacts operations.

*Acronyms: ICS: Industrial control systems; SCADA: Supervisory control and data acquisition

SOURCE: DELOITTE ANALYSIS.

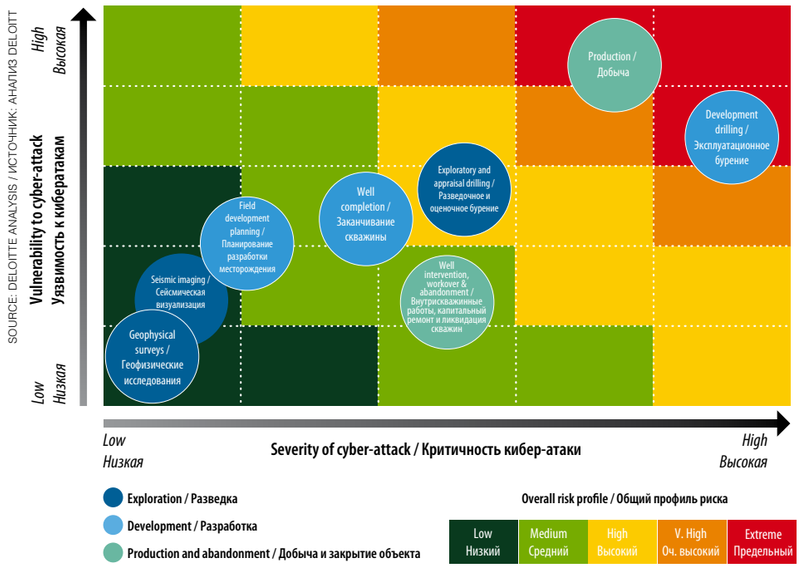
ПРОБЛЕМЫ В ЦИФРОВОЙ ОБЛАСТИ

- Комплексная экосистема: совместные операции осуществляются в разных регионах, вовлечено несколько поставщиков с различными правилами безопасности.
- Фрагментированное владение: ИТ и ОТ были разработаны с неодинаковыми целями, поэтому кибер-собственность и ответственность фрагментированы в рамках организации.
- Задержка: брандмауэры могут ввести неприемлемую задержку в критичные по времени ICS-системы, которые сталкиваются с операционными ограничениями.
- Непоследовательные кибер-стандарты: сочетание запатентованной и недавно разработанной технологии усложняет задачу.
- Нерегулярное исправление: исправление систем безопасности во многих системах является нерегулярным и зависит от поставщика в том случае, если эти системы находятся в удаленных зонах без управления человеком.
- Проблемы устаревания: многие системы имеют длительные жизненные циклы (более 10 лет), не предполагавшие обеспечения кибербезопасности. Восстановление или модернизация являются дорогостоящими и влияют на производственный процесс.

* Акронимы: ICS – промышленные системы управления; SCADA – система диспетчерского контроля и сбора данных

ИСТОЧНИК: АНАЛИЗ DELOITTE

● **Figure 2. Cyber vulnerability/severity matrix by upstream operations**
● **Рисунок 2. Кибер-уязвимость / матрица критичности для разведки и добычи**



business risks in general. It is important to note that this task requires the involvement of specialists from different fields of activity, including information technology units, with the following objectives:

Assets and equipment stocktaking, assessment of their importance for business;

Determination of the presence / absence in key assets and equipment operation of detailed vulnerabilities that can be used;

Evaluation of the maturity of means and methods for ensuring control in order to proactively manage these threats.

In addition to assessing maturity, companies should regularly dispose of some assets: those in which vulnerabilities have been identified, and those with potential security threats, advanced persistent threats (APT) or suspicious activities. It is also important to track discredited assets in advance of the occurrence of a real security threat.

Next, companies should develop a program to protect business processes and production processes. At each stage of the creation of this program, the company will increase the level of development of internal control procedures that guarantee a flexible, ready-to-run and protected control environment. Thus, the program for protecting business processes and production processes must cover three important concepts: security, readiness for threats and flexibility.

For security purposes, it is necessary to ensure systems security, or in other words to eliminate violations and prevent cracks by implementing effective automated control and monitoring tools. In addition, in the development of process control and monitoring systems, it is important to ensure clearly defined rights of access to data and the ability to monitor these rights violations.

In parallel with security, you should ensure that systems are ready for possible threats or conduct continuous monitoring to always know if the system is protected or has been compromised. To ensure that measures to

компании, происхождение экологической катастрофы, в худшем случае — гибель людей.

Для улучшения безопасности операционных процессов нефтегазовая компания должна выполнить оценку зрелости средств обеспечения контроля за информационной безопасностью производственных процессов. Следует уделять достаточное внимание анализу взаимосвязей между рисками, связанными со взломом ICS-систем, и бизнес-рисками в целом. Важно отметить, что к данной задаче требуется привлечение специалистов разных областей деятельности, в том числе подразделения информационных технологий, перед которыми будут ставиться такие цели, как:

- проведение инвентаризации активов и оборудования, оценка степени их важности для бизнеса;
- определение наличия/отсутствия в работе ключевых активов и оборудования детально изученных уязвимостей, которыми можно воспользоваться;
- проведение оценки зрелости средств и методов обеспечения контроля с целью упреждающего управления указанными угрозами.

Помимо оценки зрелости, компании должны регулярно избавляться от некоторых активов: тех, в которых были выявлены факторы уязвимости, и тех, в отношении которых обнаружены потенциальные угрозы безопасности, постоянные угрозы повышенной сложности (advance persistent threats — APT) или подозрительные действия. Также важно заблаговременно отслеживать дискредитированные активы до возникновения реальной угрозы безопасности.

Далее компаниям следует разработать программу защиты бизнес-процессов и производственных процессов. На каждом этапе создания данной программы компания будет повышать уровень развития внутренних контрольных процедур, гарантирующих гибкую, готовую к работе и защищенную контрольную среду. Таким образом, программа защиты бизнес-процессов и производственных процессов должна покрывать три важных понятия: защищенность, готовность к угрозам и гибкость.

Для защищенности необходимо обеспечивать безопасность систем, или другими словами устранять нарушения и предотвращать взломы путем внедрения эффективных автоматизированных средств контроля и мониторинга. Кроме того, при разработке систем контроля и мониторинга процессов важно обеспечивать четко определенные права доступа к данным и возможность отслеживать нарушение таких прав.

Параллельно с защищенностью следует обеспечивать готовность систем к возможным угрозам или проводить непрерывный мониторинг, чтобы всегда знать, защищена ли система или же была взломана. Для того, чтобы меры по обеспечению готовности систем к угрозам давали реальные результаты, нужно с самого начала понимать от чего необходимо защититься. Динамика киберугроз в нефтегазовом сек-

Vladimir Lasovsky, Business Development Manager, Internet of Things Business, Orange Business Services Russia and CIS

In our opinion, the first challenge Russian oil and gas companies face in ensuring cybersecurity is infrastructure aging. Large companies do not always have time to update their installed base, that is why it encounters technique with open vulnerabilities that cannot be eliminated in time before botnets or intruders build an intrusion on these published vulnerabilities.

This complexity can be divided into two separate problems. The first is the comparative simplicity and cheapness of the attack formation. You can create, for example, a distracting DDoS attack with the help of botnets, simultaneously launching an exploit and breaking into the company's information system. The second problem is the already mentioned inertia in updating the installed base in order to cover those published vulnerabilities that could lead to such an attack. At the same time, it takes much less time to form an attack than to update the equipment and software package.

The second challenge arises with an increase in the level of IT development of any production. IT development entails data-flow acquisition. Even if these data were collected earlier, it is most likely not in the same volume, or they were stored, but without any idea how to process. In fact, it is only now the understanding is shaping up that these new data, which can now be collected with the help of new digital methods and digital equipment, are of value to the business. Accordingly, only now there is an understanding that it is necessary to invest in this direction, taking into account issues of ensuring security, ensuring contours coherence, lack of access to the Internet and so on. Because of this for the most part, unprotected remote accesses are left. However, these shortcomings could be completely eliminated – you can organize secure access, provide two-factor authenticationfor employees, thereby reducing the likelihood of penetration of intruders into the circuit. For sure, well-established information systems already exist, for example, the systems with a special temporary password, but they are not widely implemented so far.

Further increase in the power of networks should inevitably lead to their integration. And here there is a third challenge: integration into general information network leads to the fact that even built-up, sufficiently protected nodes in combination with less protected objects and networks begin to lose the security factor. This leads to the fact that the segment already checked and tested from the point of view of information security needs to be checked again, because new connected segments may not have the protection set applicable to these objects. Accordingly, the possibility of data transfer, their receipt from third-party databases (for example, data transfer from one branch to another) leads to the fact that it is necessary to ensure the input of this data to the system. This very input is the vulnerability that can be used. There is an opportunity to crack not the central network, but the older one in terms of equipment and less secure in terms of functionality.

Another source of vulnerability is employees themselves. Of course, such a cyber-risk exists. For example, a person comes with his computer, tablet or smartphone, connects to the network, not knowing that he has a virus, some infected files. He can come with a flash drive, download it to an untested file from the Internet and give it to a colleague. Thus, the virus gets into the computer network. This is a common risk, it concerns not only the oil and gas sector, and companies try to make the maximum effort to minimize it.

Владимир Ласовский, менеджер по развитию бизнеса в области интернета вещей, Orange Business Services Россия и СНГ

Первая сложность, на наш взгляд, стоящая перед российскими нефтегазовыми компаниями в обеспечении кибербезопасности – это устаревшая инфраструктура. Крупные компании не всегда успевают обновлять свои парки оборудования, из-за чего в них встречается техника с уже открытыми уязвимостями, которые не успевают быть устранены прежде, чем бот-сети или злоумышленники построят вторжение на этих опубликованных уязвимостях.

Эту сложность можно разбить на две отдельные проблемы. Первая – это сравнительная простота и дешевизна формирования атаки. Можно сформировать, например, отвлекающую DDoS-атаку с помощью бот-сетей, одновременно запустив эксплоит и проникнув в информационную систему компании. Вторая проблема – это уже упомянутая инертность в обновлении парка оборудования с целью прикрытия тех опубликованных уязвимостей, которые могут привести к подобной атаке. При этом для формирования атаки нужно значительно меньше времени, чем для обновления парка оборудования и софта.

Вторая сложность возникает с повышением уровня информатизации любого производства. Информатизация влечет за собой получение потока новых данных. Даже если раньше эти данные собирались, то, скорее всего, не в том объеме, или их хранили, но не знали, как обрабатывать. По сути, только сейчас формируется понимание того, что эти новые данные, которые сейчас можно собирать с помощью новых цифровых методов и цифрового оборудования, обладают ценностью для бизнеса. Соответственно, только сейчас формируется понимание того, что в это направление необходимо инвестировать – с учетом вопросов обеспечения безопасности, обеспечения связанности контуров, отсутствия выхода в интернет и т.д. В значительной мере из-за этого остаются незащищённые удаленные доступы. Впрочем, эти недочеты вполне устранимы – можно организовать защищенный доступ, обеспечить двухфакторной аутентификацией сотрудников, тем самым уменьшив вероятность проникновения злоумышленников внутрь контура. Есть, конечно, и уже отлаженные информационные системы, например, со специальным временным паролем, но пока они внедрены не повсеместно.

Дальнейшее повышение мощности сетей неминуемо должно привести к их объединению. И здесь возникает третья сложность: объединение в общую информационную сеть приводит к тому, что даже выстроенные, достаточно защищенные узлы, которые объединяются с менее защищенными объектами и сетями, сами начинают терять коэффициент защищенности. Это приводит к тому, что уже проверенный и протестированный с точки зрения информационной безопасности сегмент нужно проверять еще раз, потому что новые подключенные сегменты могут не обладать тем спектром защиты, который предъявлялся к данным объектам. Соответственно, возможность передачи данных, их поступления из сторонних баз данных (например, передача данных от одного филиала к другому) приводит к тому, что необходимо обеспечить вход этих данных в систему. Вот этот вход и есть та самая уязвимость, которой можно воспользоваться. Возникает возможность взломать уже не центральную сеть, а более старую по оснащенности и менее защищенную по функционалу.

Еще один источник уязвимости – сами сотрудники организаций. Безусловно, такой киберриск присутствует. Например, человек приходит со своим компьютером, планшетом или смартфоном, подключается к сети, не зная, что у него есть вирус, какие-то зараженные файлы. Он может прийти с флешкой, скачать на нее непроверенный файл из интернета и отдать коллеге. Таким образом вирус попадет в компьютерную сеть. Это риск общий, он касается не только нефтегазового сектора, и компании стараются прилагать максим усилий для его минимизации.

ensure the readiness of systems to threats produced real results, it is necessary to understand from the very beginning what should be protected from. The dynamics of cyberthreats in the oil and gas sector is well traced, which gives a basic idea of what types of attacks can be carried out on ICSs of oil and gas companies. At the same time, it is necessary to understand the specifics of the business risks of a particular company in order to forecast possible incidents and design accordingly the systems for threats detecting.

For sustainability, the company must have plans and procedures for detecting, containing, neutralizing the consequences of cyberattacks and online restoring the regular mode of operation.

Indicators of risk readiness and maturity indicators of ICSs of each company vary. However, there are several fundamental means to ensure control over cyber risks, which should be available in almost every oil and gas company. The implementation of such key tools can be a starting point for the development of a special program to ensure the security and flexibility of corporate systems and their preparedness for threats. Such means include:

Conducting outreach. It is necessary to clarify the issues of cybersecurity to different company special-

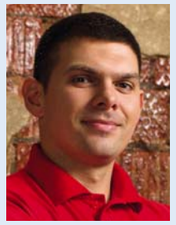
торе хорошо прослеживается, что позволяет получить базовое представление о том, какие виды атак могут производиться на ICS-системы нефтегазовых компаний. В то же время следует понимать специфику бизнес-рисков конкретной компании, чтобы спрогнозировать возможные происшествия и соответствующим образом спроектировать системы по обнаружению угроз.

Для устойчивости компания должна иметь планы и процедуры для обнаружения, сдерживания, нейтрализации последствий кибератак и оперативного восстановления штатного режима работы.

Показатели готовности к рискам и показатели зрелости ICS-систем отличаются от компании к компании. Однако, существует несколько основополагающих средств обеспечения контроля за киберрисками, которые должны быть в наличии практически у любой нефтегазовой компании. Внедрение таких ключевых средств может стать отправной точкой для разработки специализированной программы по обеспечению безопасности и гибкости корпоративных систем и их готовности к угрозам. К таким средствам относится:

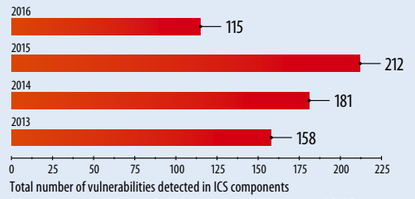
Проведение информационно-разъяснительной работы. Необходимо разъяснять вопросы кибербезопасности различным специалистам компании, а также обучать их необходимым навыкам безопасного и ответственного использования систем.

Vladimir Nazarov, Head of Industrial Control Systems Security Department, Positive Technologies

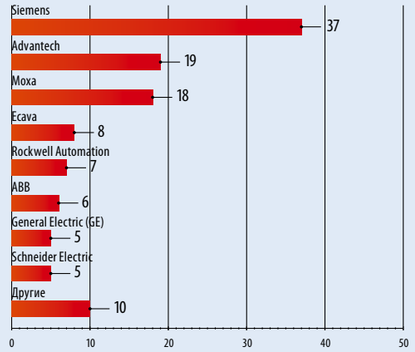


Technological progress opens new horizons to companies for management of technological and business processes, on the one hand, and, on the other hand, increases the vulnerability of enterprises to cybercriminals. Just a few years ago speaking of safety in the industrial sector and fuel and energy complex, we meant by this only physical security of facilities, now information security is coming to the fore. Advanced enterprises purposefully began to study the issues of ensuring safety of automated process control systems (APCS). The incidents with massive virus attacks (WannaCry and NotPetya) played an important role in this, which also affected industrial sector, demonstrating that the lack of proper attention to information security can lead to downtime or accidents, and lead to direct losses, sometimes amounting to millions dollars. The use of digital technologies in control systems allows the operational collection, processing and analysis of work data, which in turn allows an attacker to use the same capabilities and affect technological process. In the case of a successful attack, he will be able not only to disable expensive equipment and stop the production cycle, but also to provoke a technogenic catastrophe. In this case, you do not even need physical access to the equipment, network connection is enough.

It should be noted that the overall level of the industry security is inseparable from the safety of the equipment and software used: there is also a well-known rule that the general level of security is measured by the weakest component. And, as our studies show, the equipment used in the fuel and energy complex has a lot of vulnerabilities: in 2016 alone, more than 100 vulnerabilities were published in APCS components of the main producers. At the same time, most of them are in dispatch and monitoring devices (HMI / SCADA). And 60% has a critical and high degree of risk. The most common vulnerabilities are remote code execution, denial of service and disclosure of information, creating a risk of a hazard operation of the enterprise, breaking out of equipment, stopping production processes, which in the end is fraught with significant financial losses. As an illustrative example, we can recall the case with the malicious Industroyer, which allowed direct control of switches of electrical substations. It was the lack of protection mechanisms that made it possible to disrupt the operation of electrical substation. At the same time, one must understand that the structure of many enterprises includes power plants, where equipment is targeted by focused attacks (this is the fastest and most effective way to disrupt the enterprise operation).



Total number of vulnerabilities detected in ICS components
Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП



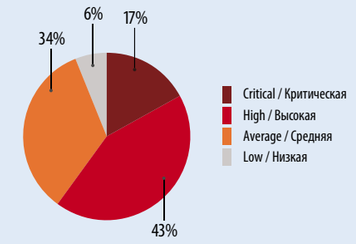
Vulnerabilities by the main manufacturers of ICS components
Уязвимости по основным производителям компонентов АСУ ТП

SOURCE: POSITIVE TECHNOLOGIES, ICS SECURITY 2016 REPORT / ИСТОЧНИК: POSITIVE TECHNOLOGIES, ИССЛЕДОВАНИЕ «БЕЗОПАСНОСТЬ АСУТП: ИТОГИ 2016 ГОДА»

Владимир Назаров, руководитель отдела безопасности промышленных систем управления Positive Technologies

Технологический прогресс открывает перед компаниями новые горизонты управления технологическим и бизнес-процессами с одной стороны, а с другой – повышает уязвимость предприятий для киберпреступников. Еще несколько лет назад говоря о безопасности в промышленном секторе и сфере ТЭК понимали исключительно физическую защиту объектов, сейчас на первый план выходит безопасность информационная. Передовые предприятия целенаправленно стали изучать вопросы обеспечения безопасности автоматизированных систем управления технологическим процессом (АСУ ТП). Не последнюю роль в этом сыграли и инциденты с массовыми вирусными атаками (WannaCry и NotPetya), которые затронули и сферу промышленности, наглядно продемонстрировав, что отсутствие должного внимания к ИБ может привести к простою производства или авариям, и вылиться в прямые убытки, исчисляющиеся иногда миллионами долларов. Использование цифровых технологий в системах управления позволяет выполнять оперативный сбор, обработку и анализ данных о работе, что в свою очередь, позволяет злоумышленнику использовать эти же возможности и влиять на технологический процесс. В случае успешной атаки он сможет не только вывести из строя дорогостоящее оборудование и остановить производственный цикл, но и спровоцировать техногенную катастрофу. При этом уже не нужен физический доступ к оборудованию, достаточно сетевого соединения.

Хочется отметить, что общий уровень защищенности отрасли неотделим от безопасности используемого оборудования и ПО: здесь также действует известное правило, по которому общий уровень безопасности измеряется по самому слабозащищенному компоненту. И, как показывают наши исследования, применяемое в сфере ТЭК оборудование имеет массу уязвимостей: только в 2016 году было опубликовано более 100 уязвимостей в компонентах АСУ ТП основных производителей. При этом большая их часть приходится на устройства диспетчеризации и мониторинга (ЧМИ/SCADA). А 60% имеет критическую и высокую степень риска. Наиболее распространенные уязвимости – удаленное выполнение кода, отказ в обслуживании и раскрытие информации, создающие риск внештатного режима работы предприятия, выхода из стоя оборудования, остановки производственных процессов, что, в конечном итоге, чревато значительными финансовыми потерями. В качестве наглядного примера можно вспомнить случай с вредоносом Industroyer, позволявшим напрямую управлять выключателями электрических подстанций. Именно отсутствие механизмов защиты позволило нарушить работу электрической подстанции. При этом надо понимать, что структура многих предприятий включает в себя энергостанции, оборудование которых становится мишенью целенаправленных атак (это самый быстрый и эффективный способ нарушить работу предприятия).



Vulnerabilities breakdown by degrees of risk level
Распределение уязимостей по степеням риска

SOURCE: POSITIVE TECHNOLOGIES, ICS SECURITY 2016 REPORT / ИСТОЧНИК: POSITIVE TECHNOLOGIES, ИССЛЕДОВАНИЕ «БЕЗОПАСНОСТЬ АСУТП: ИТОГИ 2016 ГОДА»

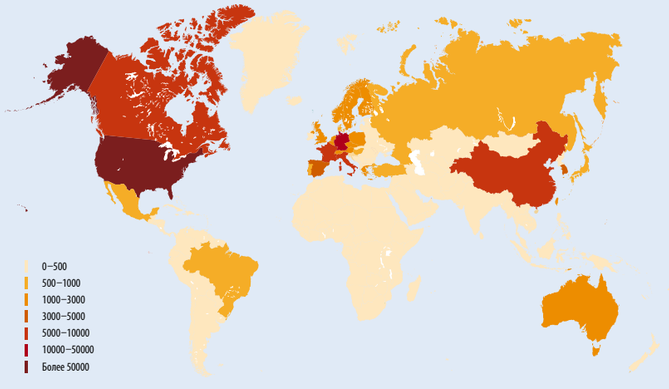
Продукты ИБ, предназначенные для промышленности, не должны влиять на технологический процесс, сетевую инфраструктуру и промышленное оборудование во избежание его отказа, снижения надежности и эффективности систем и других нежелательных последствий. Приоритет отдается непрерывности процесса, поэтому предпочтительно применение пассивных средств защиты, таких как система управления инцидентами кибербезопасности АСУ ТП. Такие решения обеспечивают непрерывный мониторинг сетевой активности и позволяют выявлять уязвимости и хакерские атаки на промышленную сеть предприятия.

Обеспечение безопасности АСУ ТП от киберугроз требует комплексного подхода. Но прежде всего мы рекомендуем выявить и устранить типовые пробелы в обеспечении безопасности, открывающие злоумышленникам возможности для проникновения в технологическую сеть. Часто в ходе анализа защищенности выясняется, что в организациях используются устаревшие версии ПО, незашифрованные протоколы, установленные по умолчанию пароли. Наиболее часто встречающаяся проблема – использование неактуальных версий ПО. Мы также часто сталкиваемся с тем, что заказчики не в полной мере владеют информацией о собственной сетевой инфраструктуре, а ведь при планировании атаки злоумышленники первым делом начинают с ее сканирования – чтобы определить все доступные для атаки устройства (в том числе и имеющие подключение к интернету – к началу 2017 года мы зафиксировали более 160 тыс. таких компонентов АСУ ТП по всему миру). Поэтому хорошей отправной точкой в начале пути по обеспечению безопасности может послужить проведение инвентаризации.

Industrial information security products should not affect the technological process, network infrastructure and industrial equipment in order to avoid its failure, reduce the reliability and effectiveness of systems and other undesirable consequences. Priority is given to the continuity of the process, therefore it is preferable to use passive protections, such as APCS cybersecurity incidents management system. Such solutions provide continuous monitoring of network activity and allow you to identify vulnerabilities and hacker attacks on the enterprise's industrial network.

Ensuring APCS protection against cyberthreats requires an integrated approach. But first of all we recommend to identify and eliminate typical security gaps that open up the possibility for malicious users to enter the technological network. Often in the analysis of security it turns out that organizations use outdated software versions, unencrypted protocols, default passwords. The most common problem is using out-of-date software versions. We also often encounter the fact that customers do not have full knowledge of their own network infrastructure, and in fact, when planning an attack, attackers first start by scanning it - to determine all the devices available to attack (including those with an Internet connection - by the beginning of 2017 we recorded more than 160 thousand such APCS components throughout the world). Therefore, an inventory can serve as good starting point on the way to ensure security.

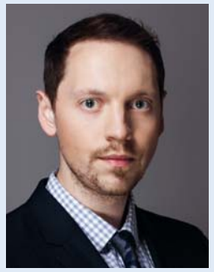
To increase the overall level of industrial systems security, it is necessary to conduct regular security analysis in order to identify possible vectors of attacks. Practice shows that this procedure should be at least annual, as during this period technology modernization of production facility can take place as well as new threats appear.



Number of ICS components available on the Internet (distribution by country)
Количество компонентов АСУ ТП, доступных в сети Интернет (распределение по странам)

SOURCE: POSITIVE TECHNOLOGIES, ICS SECURITY 2016 REPORT / ИСТОЧНИК: POSITIVE TECHNOLOGIES, ИССЛЕДОВАНИЕ «БЕЗОПАСНОСТЬ АСУТП: ИТОГИ 2016 ГОДА»

Matvey Voitov, Head of Product Marketing, Critical Infrastructure Protection Business, Kaspersky Lab



Cyber attacks on industrial facilities have long become a reality – targeted attacks, penetration of "conventional" malware into industrial networks (encryption viruses as the latest trend), fraud at the level of industrial network (the recent detention of an employee of a large corporation that is suspected of long-term concealment of traces of oil products underfilling through malware1). And this is not just news headlines; according to the recent survey of industrial cybersecurity experts2, 54% of industrial enterprises encountered at least one security incident in their ACS network. Moreover, threats are caused not only by external factors: today, both cyber attacks, failure of technological nodes, errors in industrial software, and errors of operators can disrupt the stability of production network operation.

Technological processes in each area of oil and gas complex – production, transportation and processing, distribution – now operate on the basis of automated control system, which means that the potential model of cyberthreats is similar for any industrial enterprise.

A serious difficulty is that conventional information security services are in most cases inapplicable at industrial facilities, since they do not take into account the specifics of industrial networks. Moreover, with the wrong configuration and settings, they can even be dangerous. There is a need to introduce purpose-built industrial cybersecurity solutions, which were created taking into account the threat model of APCS networks and do not have a negative impact on technological processes.

In addition to technological solutions, a significant investment in staff training is required. Often, the human factor is the key in cyberattacking. Not only in Russia, but also all over the world, people working on critical facilities are undoubtedly professionals, understand perfectly the technologies that stand behind industrial processes, but often have a low level of cybersecurity understanding. A classic example is when an employee of an enterprise brings his personal connected devices to a critical object to see something on the Internet in his spare time, then connects them to a workstation or server for charging or other purposes. In fact, he connects an isolated enterprise to an external network from within. Staff training is a zero step towards ensuring cybersecurity, for many it will become salutary.

It is no coincidence that Russian oil majors, Rosneft and Tatneft regularly train their employees at specialized industrial cybersecurity courses of Kaspersky Lab.

A feature of the oil and gas complex is the rapid adaptation of new technological solutions, primarily because of the desire to optimize costs and the availability of budgets for new technologies. The concepts of digital field and the industrial Internet of things technology type only increase the negative potential of cyberattacks. That is why it is necessary to implement an integrated approach to cybersecurity – from investing in the knowledge of employees, through auditing existing and planned for the implementation industrial technologies, to purpose-built solutions that help to prevent and detect cybersecurity incidents.

Матвей Войтов, руководитель управления продуктового маркетинга систем защиты критических инфраструктур «Лаборатории Касперского»

Кибератаки на промышленные объекты давно стали реальностью – таргетированные атаки, проникновение «традиционного» вредоносного ПО в промышленные сети (вирусы-шифровальщики, как последний тренд), мошенничество на уровне промышленной сети (недавнее задержание сотрудника крупной корпорации, который подозревается в многолетнем сокрытии следов недолива нефтепродуктов с помощью вредоносного ПО). И это не только заголовки новостей; по данным недавнего опроса специалистов по промышленной кибербезопасности 54% промышленных предприятий столкнулись хотя бы с одним инцидентом безопасности в своей сети АСУ ТП. Причем угрозы обусловлены не только внешними факторами – нарушить стабильность функционирования производственной сети сегодня могут как кибератаки, так и отказ технологических узлов, ошибки в промышленном ПО, ошибки операторов.

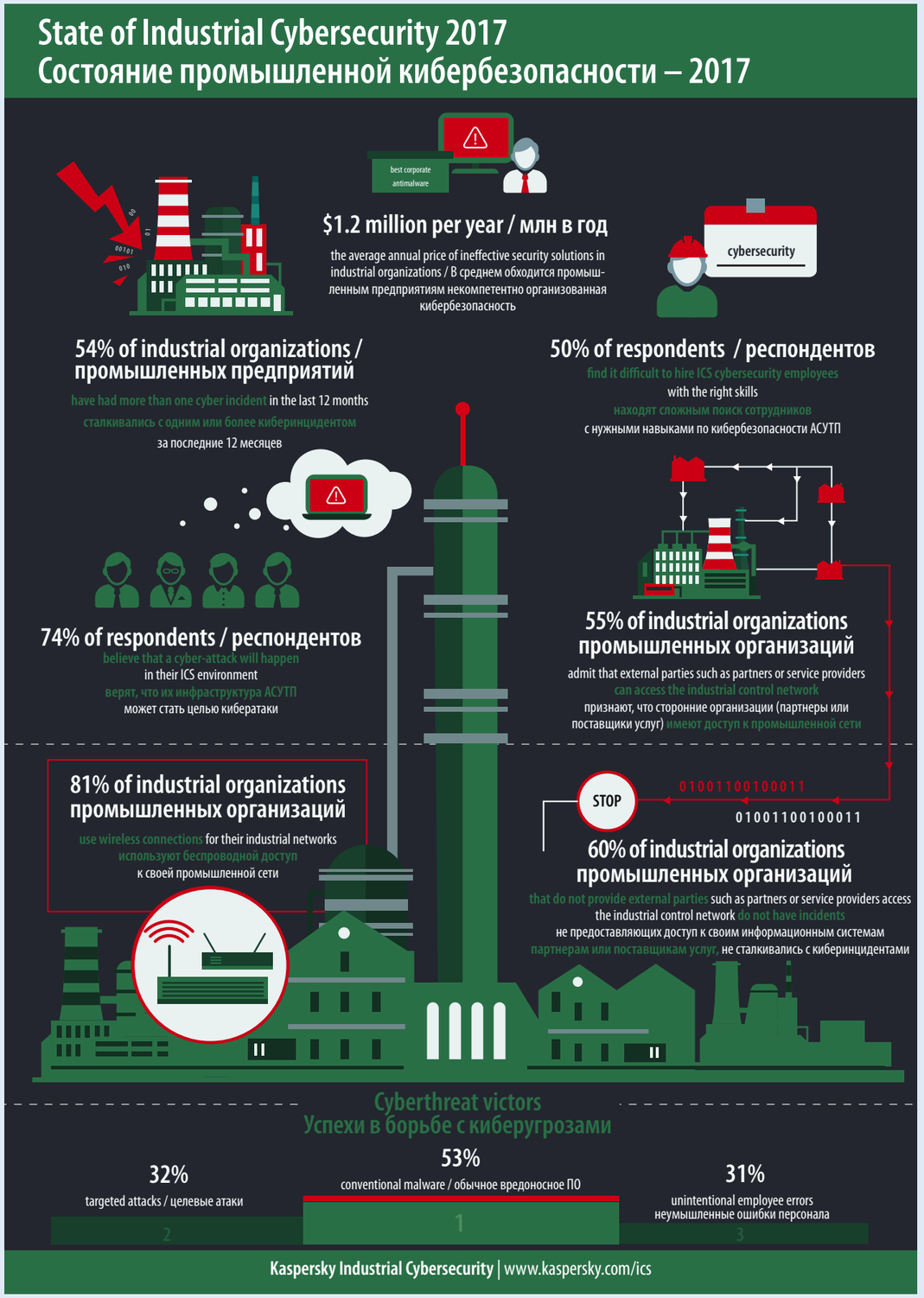
Технологические процессы в каждой отрасли нефтегазового комплекса – добыче, транспортировке и переработке, распределении – сейчас функционируют на основе АСУ, а это значит, что потенциальная модель киберугроз для любого предприятия из комплекса схожа.

Серьезной сложностью является то, что традиционные средства информационной безопасности в большинстве случае неприменимы на промышленных объектах, поскольку не учитывают специфику промышленных сетей. Более того, при неправильной конфигурации и настройке, они могут быть даже опасны. Существует необходимость внедрения специализированных решений по промышленной кибербезопасности, которые специально создавались с учетом модели угроз сетей АСУ ТП и не оказывают негативного влияния на технологические процессы.

Помимо технологических решений, необходимы значительные инвестиции в обучение персонала. Часто человеческий фактор является ключевым в кибератаке. Не только в России, но и в других странах мира люди, работающие на критически важных объектах, несомненно, являются профессионалами, отлично понимают технологии, которые стоят за промышленными процессами, но зачастую обладают низким уровнем понимания кибербезопасности. Классический пример, когда сотрудник предприятия приносит на критический объект свои личные подключенные устройства, чтобы в свободное время посмотреть что-нибудь в интернете, далее подключает их к рабочей станции или серверу для зарядки или других целей. По факту, он подключает изолированные предприятие к внешней сети изнутри. Обучение персонала – нулевой шаг к обеспечению кибербезопасности, для многих он станет спасительным.

Неслучайно, российские нефтяные лидеры, компании «Роснефть» и «Татнефть» регулярно обучают своих сотрудников на специализированных курсах по промышленной кибербезопасности от «Лаборатории Касперского».

Особенностью нефтегазового комплекса является быстрая адаптация новых технологических решений, в первую очередь из-за стремления к оптимизации затрат и наличия бюджетов на новые технологии. Концепции типа цифрового месторождения и технологии промышленного интернета вещей только усиливают негативный потенциал кибератак. Именно поэтому необходимо реализовывать комплексный подход к кибербезопасности – от инвестиций в знания сотрудников, через аудит существующих и запланированных для внедрения промышленных технологий, до специализированных решений, позволяющих предотвращать и детектировать инциденты кибербезопасности.



ists, and also teach them the necessary skills of safe and responsible systems use.

Access control. Physical and logical security of ICS components, including hardware, software applications and computer networks should be provided. Access must be provided only after the formalized authentication and authorization procedures.

Network security. Access to wired and wireless communication networks within ICS should be limited and protected, taking into account best practices in the field of identification data and access rights management. The company must perform continuous monitoring of access and authentication processes, as well as ensure the security of remote connections.

Portable media. The use of portable media within the ICS should be limited. All devices must be scanned for malicious software.

Reacting in case of incidents. The company should develop policies and procedures for managing incidents, the effectiveness of which should be periodically tested in practice.

To ensure the security of ICSs a circle of responsible persons must be defined in the company. At the same time, the functions and responsibilities of all participants in the process (from managers to equipment operators and third parties) should be clearly stated. In the end, a single order of accountability must be created. Otherwise, it will be difficult to determine uniform requirements for the whole company, and also to understand in which cases centralized or local solutions should be preferred.

Summing up, creating safe and flexible operating processes, as well as preparing for possible threats, is not an easy task for oil and gas companies. To accomplish this task, oil and gas companies must synchronize and coordinate their actions in the information and technology sphere. Solving the above problems will require the company's in-depth knowledge of information technology, as well as the best industry practices in cyber risks management. An important condition for more effective protection of operational integrity in the face of the growing number of cyber threats is the need for oil and gas companies to go beyond the traditional approach to ensure security of operational processes and implementation of reliable, flexible and ready-to-attack mechanisms.

Осуществление контроля за доступом. Должна быть обеспечена физическая и логическая безопасность компонентов ICS-систем, включая аппаратное обеспечение, программные приложения и компьютерные сети. Доступ необходимо предоставлять только после осуществления формализованных процедур аутентификации и авторизации.

Безопасность сети. Доступ к проводным и беспроводным коммуникационным сетям в рамках ICS-систем необходимо ограничить и защитить с учетом передового опыта в области управления идентификационными данными и правами доступа. Компания должна выполнять непрерывный мониторинг процессов предоставления доступа и аутентификации, а также обеспечивать безопасность удаленных соединений.

Переносные носители информации. Использование переносных носителей информации в рамках ICS-системы должно ограничиваться. Все устройства должны проверяться на предмет наличия вредоносного программного обеспечения.

Реагирование в случае возникновения инцидентов. В компании должны быть разработаны политика и процедуры управления инцидентами, эффективность которых периодически следует проверять на практике.

Для обеспечения безопасности ICS-систем в компании должен быть определен ответственный круг лиц. При этом должны быть четко прописаны функции и обязанности всех участников процесса (от менеджеров до операторов оборудования и третьих лиц). В конечном итоге должен быть создан единый порядок подотчетности. Иначе будет сложно определить единые требования для всей компании, а также понять, в каких случаях следует отдать предпочтение централизованным, а в каких локальным решениям.

Подводя итоги, создание безопасных и гибких операционных процессов, а также подготовка к возможным угрозам — непростая задача для нефтегазовых компаний. Для выполнения этой задачи нефтегазовые компании должны синхронизировать и скоординировать свои действия в информационно-технологической сфере. Решение вышеуказанных проблем потребует от компании глубокого знания информационных технологий, а также лучших отраслевых практик в области управления киберрисками. При этом важным условием для более эффективной защиты операционной целостности перед лицом растущего числа киберугроз является необходимость для нефтегазовых компаний выхода за рамки традиционного подхода к обеспечению безопасности операционных процессов и внедрения надежных, гибких и готовых к атакам механизмов.

Ruslan Stefanov, Cybersecurity Consultant, Honeywell Russia/CIS

The main cyber security issue in Russia and globally is the lack of qualified staff in the field of automatic process control system (APCS) protection (cyber defense). Big companies, including in the oil and gas industry, realize that and are concerned not only about the current shortage of cyber security personnel, but also about cyber staff leaving for service companies. To combat the shortage, companies have started to create their own security operations centers (SOCs) or have decided to contract with external ones, which allow for secure remote access to the protected assets.

By using remote access, companies avoid two additional problems associated with personnel physically being present at the sites. First, the cost of qualified specialists travelling to each site, especially if it is beyond the Arctic Circle, is very high. Second, physical presence of a specialist on the site may be less safe for the protected asset than remote access. A hacker who has physical access to the equipment has more opportunities to implement attacks.

However, the creation of SOCs implies the challenge of how to organize secure remote access from SOCs to the protected assets (sites, facilities, plants). Honeywell has already opened its own security services centers (SSC) that offer customers a set of managed security services (MSS). Honeywell also recently acquired Nextnine Ltd., a leading provider of cyber security solutions, to offer multi-vendor, multi-site secure remote access, monitoring and support to protect industrial control systems and critical infrastructure against a growing threat of cyber attacks.

The demand for such solutions and services on the Russian market is only being established. First steps on the path to adoption of the new business model of APCS protection are being taken by the Russian government and Russian businesses. This is confirmed by the new Federal Law on Security of Critical Information Infrastructure and the steps to create the GosSOPKA system (State System for Detection, Prevention and Elimination of Consequences of Cyber Attacks) as well as the creation of private SOCs.

Руслан Стефанов, консультант по защите АСУ ТП компании Honeywell в России и странах СНГ

Основная проблема, связанная с обеспечением кибербезопасности в России и мире – это нехватка квалифицированных кадров в области защиты АСУ ТП (киберзащиты). Крупные предприятия, в том числе нефтегазовые, уже осознают это и обеспокоены не только дефицитом, но и оттоком имеющихся кадров. Для того чтобы справиться с нехваткой специалистов на местах, компании стремятся централизовать компетенции и начинают создавать собственные центры обеспечения безопасности (SOC) или заключать договоры с внешними SOC других компаний. Такая централизация создает необходимость организации удаленного доступа к активам.

Наличие удаленного доступа позволяет компаниям решить несколько проблем. Во-первых, стоимость труда квалифицированных специалистов и их доставки на промышленный объект, особенно если объект расположен за полярным кругом, очень высока. Во-вторых, если на площадке отсутствует дежурный персонал, то оперативную реакцию на инциденты обеспечить затруднительно. В-третьих, личное присутствие человека на объекте может создать еще бóльшие риски для защищаемого актива, чем удаленный доступ к нему, так как злоумышленник, обладающий физическим доступом к оборудованию, имеет больше возможностей для реализации атак.

Чтобы избежать такой ситуации, когда число рисков, связанных с удаленным доступом, становится еще больше, чем без него, необходимо организовать защищенный удаленный доступ из центров обеспечения безопасности к ресурсам объектов защиты – площадок, установок, заводов. Компания Honeywell уже создала собственные центры (Security Services Centers, SSC), которые предлагают заказчикам набор услуг по управлению защитой, (Managed Security Services, MSS). Кроме этого, недавно Honeywell приобрела компанию Nextnine – ведущего поставщика и оператора решений для киберзащиты промышленных объектов. Решения Nextnine включают продукты и услуги защищенного удаленного доступа, мониторинга и поддержки.

На российском рынке спрос на такие решения только формируется. Сейчас наше государство и бизнес предпринимают очередные шаги на пути освоения новой бизнес-модели защиты АСУ ТП. Одним из таких шагов стало принятие нового Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", который даст новый толчок к созданию системы ГосСОПКА и частных SOC в России.

According to the results of Ponemon Institute

research The State of Cybersecurity in the Oil & Gas Industry: United States, Sponsored by Siemens, released on February, 2017, the deployment of cybersecurity measures in the industry isn't keeping pace with the growth of digitalization in oil and gas operations.

The purpose of this research was to understand how companies in the oil and gas industry are addressing cybersecurity risks in the operational technology (OT) environment.

In fact, just 35 percent of respondents rate their organization's operation technology (OT) cyber readiness as high. With most respondents describing their organization as having low to medium cybersecurity readiness, 68 percent of respondents say their operations have had at least one security compromise in the past year, resulting in the loss of confidential information or OT disruption.

Fifty-nine percent of respondents believe there is greater risk in the OT than the IT environment. Sixty-five percent of respondents say the top cybersecurity threat is the negligent or careless insider and 15 percent of respondents say it is the malicious or criminal insider— underscoring the need for advanced monitoring solutions to identify atypical behavior among personnel.

Only 41 percent of respondents say they continually monitor all infrastructure to prioritize threats and attacks. In fact, an average of 46 percent of all cyber attacks in the OT environment go undetected, suggesting the need for investments in technologies that detect cyber threats to oil and gas operations.

Security technologies deployed are not considered the most effective. Sixty-three percent of respondents say user behavior analytics and 62 percent of respondents say hardened endpoints are very effective in mitigating cybersecurity risks. In addition, 62 percent of respondents say encryption of data in motion is considered very effective. Yet, many companies do not have plans to deploy these technologies. Specifically, in the next 12 months less than half of organizations represented (48 percent of respondents) plan to use encryption of data in motion, only 39 percent plan to deploy hardened endpoints and only 20 percent will adopt user behavior analytics (UBA).

По результатам выпущенного в феврале 2017 года исследования

Института Понемона «Состояние кибербезопасности в нефтегазовой отрасли: Соединенные Штаты Америки» (спонсор исследования – компания «Сименс») темпы внедрение мер кибербезопасности в отрасли отстают от скорости роста цифровизации.

Целью данного исследования было выяснить, как компании нефтегазовой отрасли рассматривают проблему киберрисков в среде технологий эксплуатации (ТЭ).

Фактически только 35% респондентов оценивают готовность ТЭ своей организации к отражению кибератак как высокую. Большинство респондентов считают, что их организация имеет низкую и среднюю готовность по кибербезопасности, 68 процентов респондентов заявили, что в течение прошлого года произошло, как минимум, одно нарушение требований безопасности, что привело к потере конфиденциальной информации или нарушению ТЭ.

Пятьдесят девять процентов респондентов считают, что риск в среде ТЭ более высокий, чем в среде ИТ. 65 процентов респондентов считают, что основная угроза кибербезопасности связана с небрежностью или неосторожностью сотрудников, а 15 процентов связывают ее с внутренними злоумышленниками, подчеркивая необходимость в усовершенствованных решениях по контролю с целью выявления атипичного поведения персонала.

Только 41% респондентов отметили, что они постоянно контролируют всю инфраструктуру, чтобы ранжировать угрозы и атаки. В среднем, 46 процентов всех кибератак в среде ТЭ остаются необнаруженными, что указывает на необходимость инвестиций в технологии обнаружения киберугроз в нефтегазовой отрасли.

Применяемые технологии безопасности не считаются наиболее эффективными. Очень эффективным для снижения рисков кибербезопасности 63 процента респондентов считают использование аналитики поведения пользователей, а 62 процента – усиление защиты конечных точек. Также 62 процента респондентов считает высокоэффективным методом шифрование передаваемых данных. Тем не менее, у многих компаний нет планов по внедрению этих технологий. В частности, в ближайшие 12 месяцев менее половины представленных организаций (48 процентов респондентов) планируют использовать шифрование передаваемых данных, только 39 процентов намерены применить усиление защиты конечных точек и только 20 процентов будут использовать аналитику поведения пользователей (АПП).