ОТЧЕТ

Состояние операционных технологий и информационной безопасности

Содержание

Аннотация

Эксплуатационные технологии (OT) крайне важны для общественной безопасности и экономического благополучия: они управляют оборудованием, которое работает на производственных объектах, в энергосетях, водоснабжении, судоходстве и во многих других отраслях по всему миру.

Рост OT начался в первые десятилетия 20-го века, когда машины и устройства управления с электрическим приводом заменили оборудование, использующее силу мышц или энергию пара. OT возникли на много десятилетий раньше, чем информационные технологии (IT), при этом они всегда были изолированы друг от друга путем физического разделения. Однако в последнее время информационные технологии — датчики, машинное обучение (ML) и большие данные — объединяются с OT-сетями, чтобы обеспечить непревзойденную эффективность и конкурентные преимущества. Это увеличивает количество направлений цифровых атак и рисков вторжения.

Чтобы изучить состояние информационной безопасности в OT-средах, специалисты Fortinet провели опрос среди руководителей предприятий и операционных директоров в крупных промышленных, энергетических, коммунальных, медицинских и транспортных организациях. По результатам исследования были сделаны следующие выводы:

1. **Последствия кибератак в OT-средах обширные и глубокие.** За последние 12 месяцев около 74% OT-организаций пришлось столкнуться с вторжением вредоносных программ, которые причинили ущерб производительности, доходам, репутации бренда, интеллектуальной собственности и физической безопасности.
2. **Отсутствие эффективной системы информационной безопасности еще более увеличивает риски.** 78% респондентов имеют только фрагментарную централизованную видимость мер безопасности в своих OT-средах. 65% организаций не реализуют управление доступом на основе ролей и более половины опрошенных не используют многофакторную проверку подлинности или внутреннюю сегментацию сети.
3. **Улучшению состояния безопасности OT-систем мешают изменения, за которыми трудно угнаться, и нехватка персонала.** Почти две трети (64%) руководителей OT отмечают, что они с трудом успевают за изменениями и почти половина (45%) испытывает недостаток в квалифицированных кадрах.
4. **Организации все чаще задумываются об информационной безопасности OT.** 70% планируют развернуть систему информационной безопасности OT под руководством начальника отдела информационной безопасности в следующем году (только 9% опрошенных руководителей отделов безопасности в настоящее время осуществляют контроль за безопасностью OT-систем). В 62% организаций увеличили бюджет на информационную безопасность.

В этом отчете приводятся результаты опроса, в том числе:

- проблемы, с которыми сталкиваются руководители предприятий, когда разрабатывают защиту для своих OT-сред;
- виды и последствия вторжений угроз, которые они испытывают;
- как они управляют информационной безопасностью;
- с какими слабыми местами в системе безопасности сталкиваются;
- как измеряют успешность принятых мер.

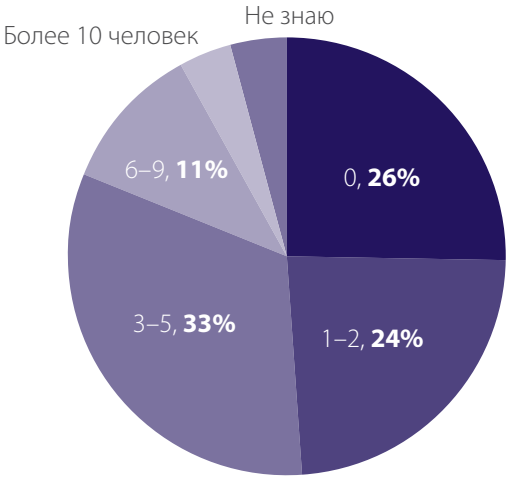
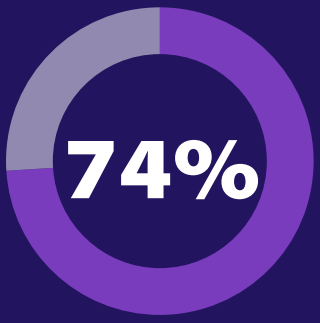
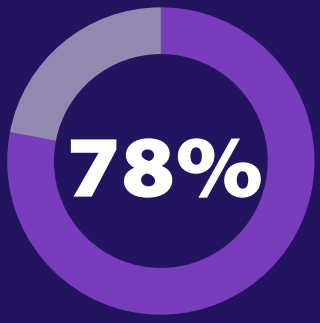


Рис. 1: количество вторжений в последние 12 месяцев

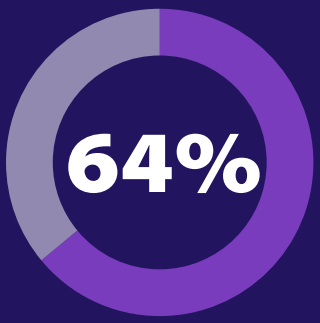
Инфографика: основные выводы по информационной безопасности OT



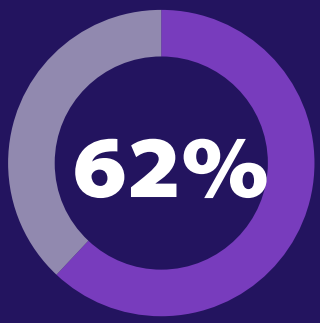
OT-организаций, принявших участие в опросе, столкнулись за последние 12 месяцев с нарушениями безопасности, которые привели к потере данных, перебоям в работе или простоям и/или снижению производительности.



имеют ограниченную централизованную видимость мер информационной безопасности.



с трудом успевают за изменениями.



увеличивают бюджет на информационную безопасность в своих организациях.

Вторжение нанесло ущерб

- Производительность (43%)
- Доходы (36%)
- Репутация бренда (30%)
- Уязвимые бизнес-данные (28%)
- Риск физической безопасности (23%)

70% планируют **развернуть систему информационной безопасности под руководством начальника отдела информационной безопасности** в следующем году.

Однако только 9% руководителей отделов безопасности контролируют информационную безопасность OT-систем уже сейчас.

По сравнению с OT-организациями нижнего уровня (больше 6 вторжений за 12 месяцев) OT-организации верхнего уровня (0 вторжений за 12 месяцев):

100% чаще используют многофакторную проверку подлинности;

94% чаще используют управление доступом на основе ролей;

68% чаще осуществляют управление и мониторинг событий безопасности и анализ событий

51% чаще используют сегментацию сети;

46% чаще планируют проверки соответствия системы безопасности стандартам.

Методология исследования

Отчет о состоянии эксплуатационных технологий и информационной безопасности составлен по данным опроса, проведенного в январе 2019 года. В опросе участвовали лица, которые:

- работают в производственной, энергетической, коммунальной, медицинской или транспортной отрасли, в компании, насчитывающей более 2500 сотрудников;
- непосредственно отвечают за эксплуатационные технологии;
- должны отчитываться за результаты работы;
- имеют отношение к принятию решений о покупках, связанных с информационной безопасностью.

Выводы о безопасности ОТ-операций

Вывод: последствия кибератак в ОТ-системах являются тяжелыми и затрагивают множество аспектов

Почти три четверти (74%) ОТ-организаций испытали как минимум одно вторжение вредоносной программы за прошедший год, а половина (50%) испытали от 3 до 10 вторжений.

Как показано на рис. 2, вредоносные программы являются преобладающей формой вторжений, далее следует фишинг (45%), шпионские программы (38%) и нарушения безопасности мобильных устройств (28%).

Последствия нарушений безопасности в ОТ-организациях являются тяжелыми, как показано на рис. 3.

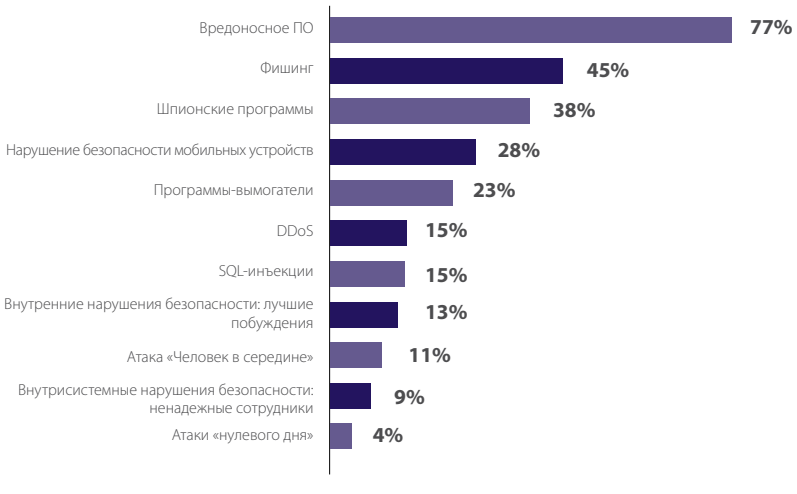


Рис. 2: виды вторжений в ОТ-системы

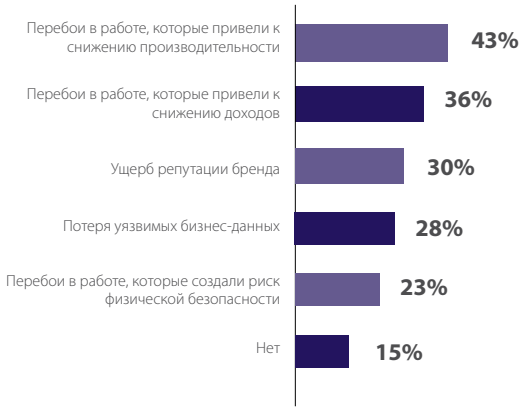


Рис. 3: последствия нарушений безопасности в ОТ-организациях

Вывод: отсутствие видимости мер информационной безопасности увеличивает риски

78% организаций имеют только фрагментарную видимость OT-операций, как показано на рис. 4.

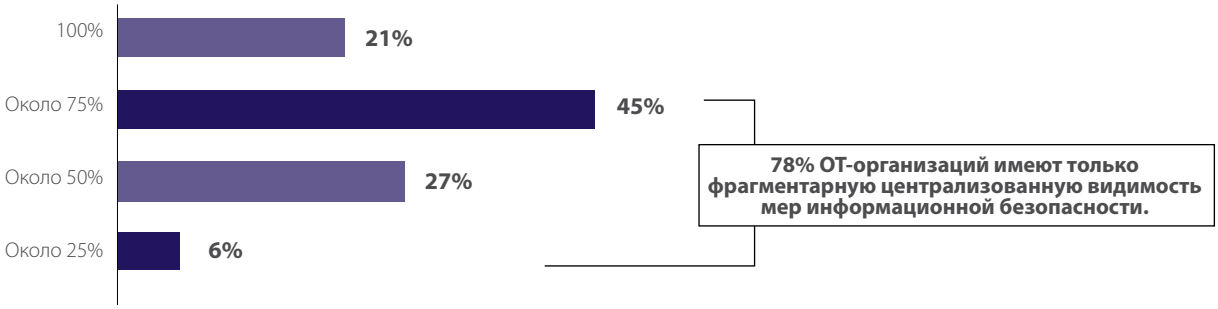


Рис. 4: процент центральной видимости мер информационной безопасности

Вывод: нехватка квалифицированных кадровых ресурсов замедляет улучшение состояния информационной безопасности

Почти две трети руководителей предприятий (64%) отмечают, что им трудно успевать за изменениями, что влечет за собой дополнительные проблемы:

- Отношения с профессиональными союзами (45%)
- Нехватка квалифицированных кадров (45%)
- Изменения в регулировании (44%)
- Возможность и доступ к обучению (42%)
- Бюджетные ограничения (42%)

Кроме того, нехватка квалифицированной рабочей силы является одним из факторов, вызывающих беспокойство у руководителей предприятий в связи с внедрением решений информационной безопасности:

- Создает дополнительную сложность (53%)
- Требует сложной адаптации стандартов безопасности (45%)
- Требует дополнительного эксплуатационного персонала (45%)
- Препятствует оперативной гибкости (44%)

Однако, согласно дополнительным данным, несмотря на нехватку кадровых ресурсов, OT-организации стремятся улучшить состояние безопасности. На рис. 5 показаны основные понятия, которые перечислили руководители предприятий в ответ на вопрос о том, какие проблемы заставляют их улучшать состояние информационной безопасности.

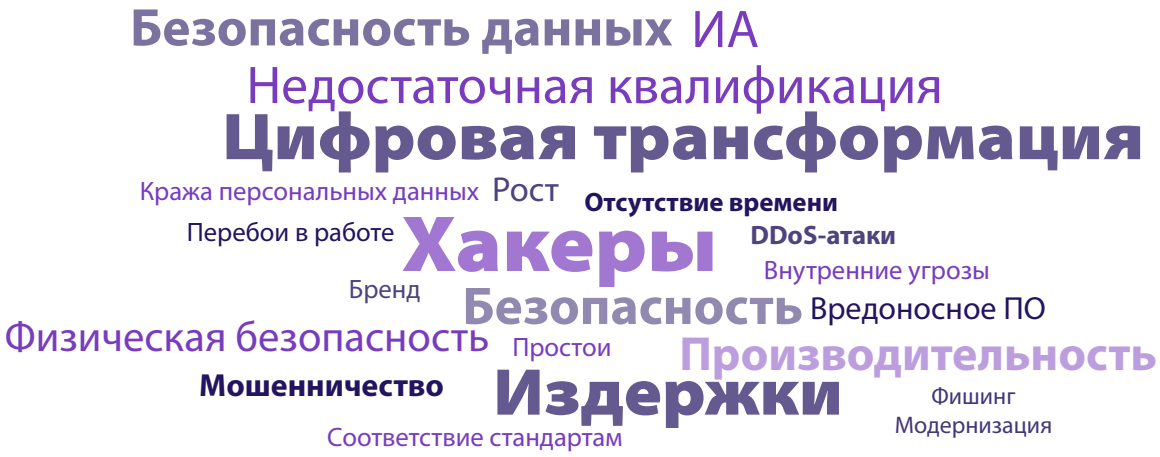


Рис. 5: основные проблемы, способствующие повышению уровня информационной безопасности

Вопрос, который лежит в основе рис. 5: «Какие три проблемы заставляют вас улучшать или изменять состояние информационной безопасности в вашей организации?». Чем чаще понятие появлялось в ответах респондентов, тем больший размер оно имеет на рисунке.

Наиболее частые проблемы безопасности, которые руководители предприятий выражают на рис. 5, — это возможность помешать хакерам, обеспечить снижение роста направлений атак, вызванного цифровой трансформацией, следить за безопасностью данных и поддерживать безопасность, производительность, рентабельность и соответствие стандартам для своих сред — и при этом постоянно испытывать нехватку квалифицированных сотрудников.

Вывод: в OT-организациях все чаще задумываются об информационной безопасности

70% организаций, принявших участие в опросе, планируют развернуть систему информационной безопасности OT под руководством начальника отдела информационной безопасности в следующем году. Интересно, что только 9% руководителей отделов информационной безопасности в настоящее время контролируют информационную безопасность OT. Сейчас в 50% организаций за информационную безопасность OT отвечает директор или инженер по информационной безопасности, а еще 24% заявили, что информационной безопасностью занимается вице-президент или директор по сетевым технологиям и операциям.

Приоритезация информационной безопасности проявляется не только в организационной реструктуризации обязанностей. **62% организаций отмечают, что их бюджеты на информационную безопасность в этом году значительно увеличились,** тогда как 38% сохранили текущие бюджеты. Организации OT уделяют особое внимание рискам информационной безопасности: 94% респондентов говорят, что они включают состояние безопасности OT как существенный или умеренный фактор риска в расширенный список рисков, который руководитель отдела безопасности обсуждает с руководителями или советом директоров.

Вывод: защита OT-сред отличается сложностью

OT-среды, над защитой которых работают респонденты, являются сложными. Они состоят из большого количества устройств OT, от 50 до более чем 500, как показано на рис. 6.

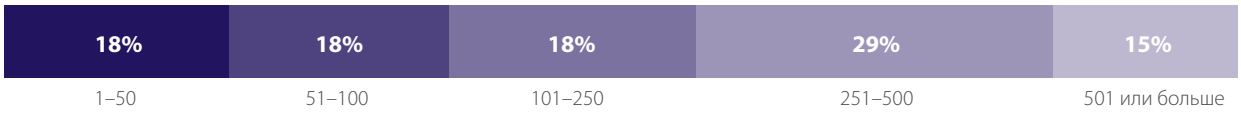


Рис. 6: количество OT-устройств в эксплуатации

Большинство организаций приобретают свои устройства у 2–4 поставщиков, как показано на рис. 7.

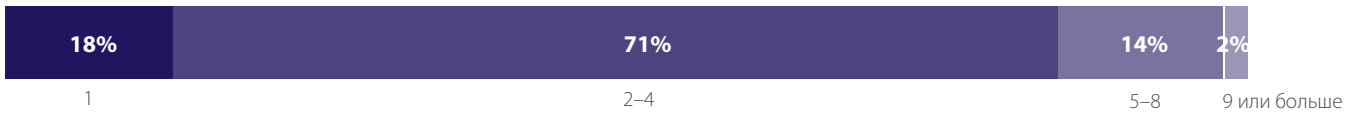


Рис. 7: количество поставщиков OT-устройств

Чаще всего респонденты упоминали таких поставщиков OT-устройств, как Honeywell, Siemens и Emerson (см. Рис. 8).

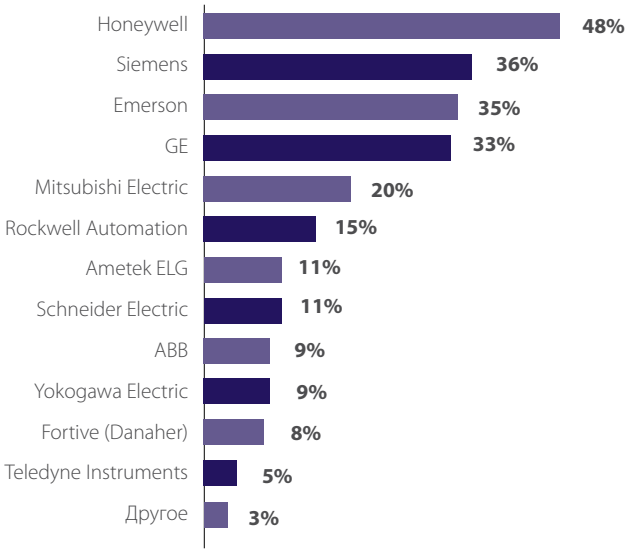


Рис. 8: поставщики OT-устройств

Вывод: руководители предприятий оказывают влияние на повышение уровня информационной безопасности

По мере того как OT-организации усиливают информационную безопасность своих сред, руководители предприятий активно участвуют в принятии решений. Более трех четвертей (76%) сообщают, что они регулярно участвуют в принятии решений по информационной безопасности, и почти половина (45%) отмечают, что при принятии решений по безопасности OT решающее слово остается за ними. Почти все регулярно (56%) или иногда (39%) участвуют в разработке стратегии информационной безопасности ИТ-систем своей организации.

Интересно отметить, что безопасная и стабильная среда имеет важное значение для трех основных показателей успеха, по которым оцениваются руководители предприятия: максимизация производительности (55%), минимизация затрат (53%) и сокращение времени реагирования на уязвимости безопасности (44%).

Может показаться удивительным, что «сокращение времени реагирования на уязвимости безопасности» является третьим по важности показателем успеха. Но представьте, как быстро кибератака может нарушить работу таких объектов, как фабрика, коммунальное предприятие или железная дорога, причинив ущерб производительности, доходам и безопасности.

Угроза кибератаки вызывает серьезное беспокойство, и мы инвестируем в мероприятия, позволяющие ее предотвратить.

– Операционный директор, производственнаякомпания

Стабильная и отказоустойчивая среда также имеет решающее значение для трех основных служебных обязанностей руководителей предприятий: управление эффективностью производства (77%), контроль работы сотрудников (77%) и управление контролем качества и производственными процессами (76%).

Учитывая то внимание, которое они уделяют стабильности и отказоустойчивости, становится более очевидным, почему 76% руководителей предприятий активно участвуют в решении вопросов по информационной безопасности OT. Эта задача потребует больше времени, так как, согласно прогнозам, расходы на информационную безопасность OT вырастут на 50% и достигнут суммы в 18,05 млрд долларов в 2023 году по сравнению с 12,22 млрд долларов в 2017 году. [1]

Существует ряд недостатков в системе информационной безопасности, которые должны исправить сотрудники OT, как показано в следующем разделе.

Вывод: в механизмах управления доступом, проверки подлинности, сегментации сетей и других есть узкие места

На рисунке 9 показано, сколько процентов OT-организаций не используют перечисленные ниже основные функции безопасности.

Рис. 9: процент OT-организаций, не использующих основные меры безопасности, в том числе информационной

Неиспользуемые функции, показанные на рис. 9, приводят к возникновению узких мест в безопасности:

- **Около двух третей (65%)** OT-компаний не используют управление доступом на основе ролей, что дает злоумышленникам большую свободу перемещений в их OT-средах.
- **Почти 6 из 10** (56%) OT-организаций не используют многофакторную проверку подлинности. В последнем отчете компании Verizon сообщается, что 81% нарушений безопасности начинается с кражи учетных данных.[2] Многие нарушения безопасности в OT рассчитаны на получение учетных данных посредством фишинга. (Согласно оценке *Wall Street Journal*, в течение двух последних лет около двух десятков американских энергетических компаний были взломаны с использованием фишинга и украденных учетных данных, причем злоумышленники оставили в скомпрометированных OT-средах вредоносные программы, которые планировали использовать для будущих диверсий. [3]) Многофакторная аутентификация затрудняет успешное использование украденных учетных данных.
- **Более половины** организаций (53%) не имеют внутренней сегментации сети. В Руководстве по информационной безопасности Национального института стандартов и технологий (NIST) сегментация названа «одной из наиболее эффективных архитектурных концепций, которую организация может реализовать» для защиты своей OT-среды. [4] Отраслевые эксперты отмечают, что многие недавние атаки вредоносных программ на OT-сети можно было предотвратить с помощью сегментации, так как сегментация ограничивает свободу перемещения из одной производственной OT-сети в другую и даже внутри одной производственной OT-сети. [5]
- **Почти половина** (44%) организаций не имеет центра операций безопасности (SOC) и более половины (55%) не имеют центра операций сети (NOC), что приводит к снижению видимости и росту рисков. Центр SOC может быстро обнаружить, предотвратить или минимизировать нарушение безопасности. NOC максимизирует пропускную способность и готовность сети. SOC и NOC можно интегрировать в одну систему, чтобы улучшить результаты обоих центров. [6]
- **Почти 4 из 10 организаций** (39%) не управляют событиями безопасности, не ведут их мониторинг или анализ, что затрудняет обнаружение нарушений безопасности. Поскольку в настоящее время большинство организаций признают неизбежность вторжений, критически важным фактором для минимизации последствий нарушения безопасности является киберустойчивость, или реагирование на инциденты и управление событиями. [7]
- Базовые методы обеспечения безопасности остаются трудной задачей для значительного количества организаций, при этом **треть** (33%) респондентов признает что у них нет программ повышения осведомленности и обучения по вопросам внутренней безопасности. Поскольку внутрисистемные угрозы составляют 30% всех нарушений, это необходимо для любой организации, как ИТ, так и OT. [8]

Передовой опыт OT-организаций верхнего уровня

26% наших респондентов (организации «верхнего уровня») сообщают **об отсутствии вторжений** за последние 12 месяцев. Напротив, 17% респондентов (организации «нижнего уровня») имели **шесть или более** вторжений за последние 12 месяцев, а некоторые даже не знают, сколько вторжений у них было. Интересно отметить следующие несоответствия между этими двумя группами.

1. **Организации верхнего уровня на 100% чаще, чем организации нижнего уровня, используют многофакторную проверку подлинности,** что затрудняет доступ с украденными учетными данными.

2. **Организации верхнего уровня на 94% чаще, чем организации нижнего уровня, используют управление доступом на основе ролей,** ограничивая возможности перемещений для потенциальных хакеров.

3. **Организации верхнего уровня на 68% чаще, чем организации нижнего уровня, управляют событиями безопасности и осуществляют их мониторинг, а также выполняют анализ событий,** тем самым снижая риск нарушений безопасности путем минимизации времени на обнаружение вторжения.

4. **Организации верхнего уровня на 51% чаще, чем организации нижнего уровня, используют сегментацию сети,** ограничивая возможности перемещений для потенциальных хакеров.

5. **Организации верхнего уровня на 46% чаще, чем организации нижнего уровня, планируют ревизии соответствия стандарту системы безопасности**, чтобы усилить безопасность.

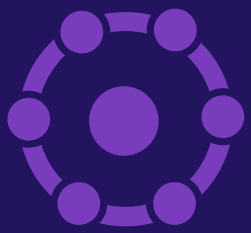
Заключение: информационная безопасность становится необходимостью для успешной работы OT-систем

OT-среды характеризуются высоким риском: почти 8 из 10 организаций столкнулись с нарушениями безопасности в прошлом году, при этом половина респондентов заявляет, что нарушений было от 3 до 10 или даже больше. Сообщается, что в результате этих нарушений был нанесен ущерб производительности, доходам, доверию к бренду, интеллектуальной собственности и физической безопасности. В данном исследовании идентифицируются факторы, которые необходимо рассмотреть для снижения рисков. Например, тот факт, что 78% организаций не имеют централизованной видимости мер информационной безопасности, 56% не используют многофакторную проверку подлинности, а 53% все еще не использует внутреннюю сегментацию сети, которую рекомендуется использовать в OT- сетях. [9]

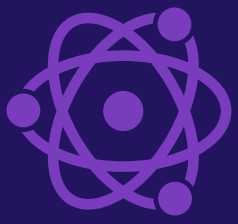
Руководители предприятий рассказали о своем участии в оценке решений информационной безопасности и о своем влиянии на принятие решений по этим вопросам. Они ищут решения, которые соответствуют их основным задачам по максимизации производительности с минимальными затратами.

Чтобы решить проблему отсутствия централизованной видимости и нехватки кадровых ресурсов, OT-организации должны прислушаться к следующим рекомендациям.

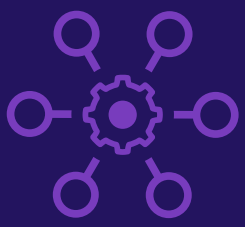
> ***«Решения обеспечения безопасности должны действовать интеллектуальнее и быть более эффективными, часто в рамках уменьшенного бюджета».***
>
> – Вице-президент по производству, крупная производственная компания



Ищите решения обеспечения безопасности, которые работают совместно и обеспечивают широкую видимость направлений цифровых атак благодаря объединению сред OT и IT.



Рассмотрите подход на основе адаптивной системы сетевой безопасности, которая предоставляет комплексную защиту всех устройств, сетей и приложений.



Ищите автоматизированные средства обеспечения безопасности с решениями, которые координируют отклик и используют такие технологии, как машинное обучение.

Минимизируйте риски с помощью таких рекомендованных методов, как сегментация сети, многофакторная проверка подлинности и управление доступом на основе ролей.

Эти принципы информационной безопасности улучшат состояние безопасности в вашей организации и помогут компенсировать нехватку кадровых ресурсов.

Справочные материалы

[1] Industrial Control Systems (ICS) Security Market worth $18.05 billion by 2023, MarketsandMarkets, по состоянию на 25 февраля 2018 г.

[2] 2017 Data Breach Investigations Report, Verizon, по состоянию на 30 ноября 2018 г.

[3] Ребекка Смит (Rebecca Smith) и Роб Барри (Rob Barry), America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It, The Wall Street Journal, 10 января 2019 г.

[4] Кейт Стуфер (Keith Stouffer) и др., Guide to Industrial Control Systems (ICS) Security, NIST, майт 2015 г.

[5] Питер Ньютон (Peter Newton), Securing IIoT requires extra care. NAC and segmentation can help, TechTarget, 28 сентября 2018 г.

[6] Bridging the NOC-SOC Divide, Fortinet, по состоянию на 5 марта 2019 г.

[7] Patrick Spencer, Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study, Scalar Security Blog, 20 февраля 2019 г.

[8] 2018 Data Breach Investigations Report, Verizon, март 2018 г.

[9] Кейт Стуфер (Keith Stouffer) и др., Guide to Industrial Control Systems (ICS) Security, NIST, май 2015 г.

FORTINET

www.fortinet.com/ru

августа 28, 2019 11:22 AM

330327-0-1-RU

Z:_argostranslations\130\03_DTP\Manufacturing-Plant Operations\report-state-of-operational-technology-A4_RU