УДК 004.512.4

КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ПРОИЗВОДСТВЕ

И.Д. Алекперов

к.т.н., доцент

магистрант 2 года обучения

ЧОУ ВО ЮУ (ИУБиП)

e-mail: ilgar@iubip.ru

А.Р. Дмитриева

магистрант 2 года обучения

ЧОУ ВО ЮУ (ИУБиП)

e-mail: a.dm3008@yandex.ru

Д.Е. Вегерин

студент 4 года обучения

ЧОУ ВО ЮУ (ИУБиП)

e-mail: domask138@gmail.com

Аннотация: Понятие кибербезопасности подразумевает под собой совокупность методов, технологий и процессов, предназначенных для защиты целостности сетей, программ и данных от цифровых атак. Целью кибератак является получение несанкционированного доступа к конфиденциальной информации ее копирование, изменения или уничтожение. Так же могут служить для вымогательства денежный средств у пользователей или нарушения рабочих процессов в компании.
Ключевые слова: кибербезопасность, кибератаки, интернет, сети, системы, правоохранительные органы.

CYBER SECURITY OF AUTOMATED SYSTEMS IN MANUFACTURING

I. D. Alekperov

A. R. Dmitrieva

D. E. Vegerin

Abstract: The concept of cybersecurity implies a set of methods, technologies and processes designed to protect the integrity of networks, programs and data from digital attacks. The purpose of cyber attacks is to gain unauthorized access to confidential information by copying,

modifying or destroying it. They can also serve to extort money from users or disrupt business processes in the company.
Keywords: cybersecurity, cyber attacks, Internet, networks, systems, law enforcement.

Риски кибербезопасности усиливаются во всех сферах, связанных с технологиями. И, похоже, с тем же темпом, с которым развиваются сами технологии. В последние несколько лет отрасль производства регулярно сталкивается с киберугрозами. Их сложность и интенсивность возрастают с каждым днем. Хотя организации вкладывают в обеспечение информационной безопасности все больше сил, хакеры все равно находят способы проникать за их периметр и похищать конфиденциальную и иную критически важную информацию, включая персональные данные работников и производственные секреты

По мере совершенствования технологий, применяемых на предприятии, будут усложняться и киберугрозы. Учреждениям в области производства придется столкнуться с еще более значительными проблемами, чем сегодня: как только появляется новая технология, нейтрализующая цифровые угрозы.

Автоматизированные системы управления технологическим процессом (АСУ ТП) во многом отличаются от обычных производственных информационных систем: начиная с назначения, специальных протоколов передачи данных, используемого оборудования, и заканчивая средой, в которой они функционируют. В традиционных системах объектом защиты является информация, которая передаётся, хранится и обрабатывается, и целью является ограничение несанкционированного доступа к ней. В АСУ ТП же защищается сам процесс производства, и главная цель обеспечение его непрерывности и целостности. При нарушении производственного процесса могут пострадать как производимая продукция, так и обслуживающий персонал, инфраструктура и экосистема.

Существует множество заблуждений насчёт АСУ ТП, такие, как: «АСУ ТП изолированы от внешних сетей», «АСУ ТП слишком необычны, чтобы их могли взломать», «Никто не хочет взламывать АСУ ТП» и т.д. Многие

автоматизированные системы в той или иной степени имеют выход во внешние сети, и иногда даже владельцы не знают об этом. Это значительно упрощает задачу для хакеров. Однако, это не единственный способ. Как правило, системы хранения и передачи данных автоматизированных систем очень плохо защищены, и не составляет труда их взломать. Об этом говорят данные многих проверок на безопасность и отчёты специалистов.

Кибербезопасность АСУ ТП во многом похожа на информационную безопасность обычных систем, но там существует много мелких различий. Ей так же присущи многие похожие процессы, такие, как: реагирование на угрозы, постоянный мониторинг состояния системы, управление безопасностью и т.д. Хотя процессы и похожи, всё же они разные.

Современный опыт решения проблем кибербезопасности показывает, что для достижения наибольшего эффекта при организации защиты технического процесса необходимо руководствоваться рядом принципов.

Первым и наиболее важным является принцип непрерывного совершенствования и развития системы кибербезопасности. Суть этого принципа заключается в постоянном контроле функционирования системы, выявлении ее слабых мест, потенциально возможных каналов проникновения злоумышленников, обновлении и дополнении механизмов защиты в зависимости от изменения характера внутренних и внешних угроз, обосновании и реализации на этой основе наиболее рациональных методов, способов и путей защиты технического процесса. Таким образом, обеспечение кибербезопасности не может быть одноразовым актом.

Вторым является принцип комплексного использования всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла.

Кроме того, наибольший эффект достигается в том случае, когда все используемые средства и методы объединяются в единую систему кибербезопасности. Только в этом случае появляются свойства, не присущие ни одному из отдельных элементов системы защиты, а также появляется

возможность управлять системой, её ресурсами и применять необходимые методы защиты.

Важнейшими условиями обеспечения безопасности являются законность, достаточность, высокий уровень подготовки представителей службы информационной безопасности, подготовка пользователей и обслуживающего персонала, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

Без соблюдения этих условий никакая система кибербезопасности не может обеспечить требуемого уровня защиты.

Рассматривая возможные угрозы, в первую очередь выделяют угрозы, связанные с неполадками в программном обеспечении, вызванные либо случайными сбоями, либо внешним воздействием через какие-либо точки доступа. В качестве таких точек могут выступать как сопряжённые корпоративные сети, интернет, так и пункты управления самой АСУ.

В настоящее время количество обнаруженных уязвимостей АСУ с каждым годом всё возрастает. В 2015 году было опубликовано 189 уязвимостей, многие из которых имеют критический характер. Все они могут быть использованы злоумышленниками для проникновения, ведь к 26 из 189 опубликованных есть известные способы проникнуть в систему. Наибольшее число уязвимостей было обнаружено в устройствах Siemens, Schneider Electric и Hospira.

Для 85% ошибок 2015 года доступны патчи и новые версии прошивки, остальные же не получили должного обслуживания. Эти уязвимости представляют большую угрозу для тех, кто использует соответствующие системы. Некоторые уязвимые места в результате ошибок оказались доступны через интернет. Например, 11 904 интерфейса удалённого управления солнечными панелями, у которых из-за отсутствия постоянно заменяемых паролей велик риск взлома.

Основные угрозы кибербезопасности (киберугрозы)

Угрозы безопасности формируются быстрее, чем наше представление о возможном риске в том или ином аспекте системы. То, что раньше не представляло никакой опасности - сегодня может оказаться весьма серьезной и критической проблемой. Тем не менее, есть ряд общеизвестных угроз о которых стоит помнить и применять меры соответствующей защиты для предотвращения их возникновения.

Пять базовых мер обеспечения кибербезопасности на предприятии

1. Исключить подключение АСУ ТП к сети Интернет.Поскольку большинство SCADA-систем не имеют адекватных средств защиты от киберугроз, важно исключить их включение в глобальную сеть Интернет и в корпоративные сети предприятий. Если же подключение к этим сетям предусмотрено, тогда требуется применение межсетевых экранов, систем обнаружения вторжения и других мер для защиты от несанкционированного доступа.

2. Избегать «дефолтных» конфигураций. Это требование применимо как к прикладным системам и сетевой инфраструктуре, так и к используемым средствам защиты от киберугроз. Должна производится замена заводских паролей (паролей по-умолчанию); они должны быть достаточно надежными, и также должно быть предусмотрено их регулярное изменение.

3. Использовать средства проверки и блокировки использования флеш-накопителей и переносных жестких дисков. Когда система отключена от внешних сетей, единственный маршрут попадания в нее зловредного ПО - через флеш-накопители и другие внешние носители. Поскольку такой способ атаки является основным, когда речь идет о изолированных системах, важным аспектом является развертывание системы сканирования внешних носителей на предмет наличия угроз.

4. Обеспечить защиту от зловредного ПО, находящегося в «спящем» режиме. Часто зловредное ПО, уже попавшее в систему, никак себя не проявляет. До некоторой поры. Поэтому важно применять системы,

позволяющие сканировать файлы с использованием нескольких антивирусных движков.

5. Обеспечить выполнение тестовых атак для оценки уязвимостей системы. Лучше, если такие атаки будет проводить третье лицо по вашему заказу, что позволит взглянуть на уровень защищенности системы объективно.

В заключение можно сказать, что только комплексный подход к обеспечению безопасности сможет защитить системы управления от взломов, сбоев и ошибок.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алекперов И.Д. Электронная коммерция (E-commerce). LAP LAMBERT Aca-demic Publishing. ISBN 978-3-330-35282-7, URN: 101:1-201708141845, EAN: 9783330352827 http://d-nb.info/Erschei-nungsdatum: 2017 г.

2. Алекперов И.Д. Разработка информационного ресурса выпускников “Школы развития личности и успеха ИУБиП” в интернет пространстве с использованием языков программирования PHP, MySQL. Ростов-на-Дону: Институт управления, бизнеса и права, 2013 г.

3. Алекперов И.Д. Электронный бизнес-консалтинг как средство развития региональной электронной коммерции // Интеллектуальные ресурсы - региональному развитию. – 2016. – № 2. – С. 6-9.

4. Витченко О.В. Современные подходы к организации самостоятельной работы обучающихся в профессиональном образовании. – Ростов-на-Дону: Изд-во «АкадемЛит», 2016. – 108 с.

5. Витченко О.В. Трансформация функций информационной системы вуза как условие его развития в региональном образовательном кластере // Интеллектуальные ресурсы - региональному развитию. – 2016. – № 2. –С. 20-24.

6. «Информационный взрыв» XXI века, или Горе от ума. [Электронный ресурс]. URL: http://for-ua.com/.../080854.html (Дата обращения 23.01.2017 г.)