

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

В. В. Подтопельный

КИБЕРБЕЗОПАСНОСТЬ АСУТП

Учебно-методическое пособие по изучению дисциплины
для студентов по специальности
10.05.03 «Информационная безопасность автоматизированных систем»,
специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.056(076)

Рецензент

кандидат физико-математических наук, доцент, доцент кафедры
информационной безопасности института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»
Н. Я. Великите

Подтопельный, В. В.

Кибербезопасность АСУТП: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем» / В. В. Подтопельный. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 39 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Кибербезопасность АСУТП». Содержит характеристику дисциплины (цель и планируемые результаты изучения дисциплины, место дисциплины в структуре основной профессиональной образовательной программы, описание видов и процедур текущего контроля и промежуточной аттестации), тематический план с описанием для каждой темы форм проведения занятия, вопросов для изучения, методических материалов к занятию, методических указаний по выполнению самостоятельной работы.

Табл. 2, список лит. – 21 наименование

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 26 мая 2025 г., протокол № 4

УДК 004.056(076)

© Федеральное государственное
бюджетное образовательное
учреждение высшего образования
«Калининградский государственный
технический университет», 2025 г.
© Подтопельный В. В., 2025 г

ОГЛАВЛЕНИЕ

Введение.....	4
1. Тематический план.....	6
2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ	8
Раздел 1. Методы защиты ПО	8
Тема 1.1 Специфика инцидентов ИБ в АСУТП. Протоколы АСУТП.	8
1. Особенности АСУТП и риски киберинцидентов.....	8
2. Уязвимости промышленных протоколов	8
3. Основные угрозы для АСУТП	9
4. Методы защиты промышленных систем.	9
5. Нормативная база и стандарты:	9
6. Будущее безопасности АСУТП:	9
Тема 1.2 Методы защиты ПО АСУТП.	11
Тема 1.3 Методы и средства исследования ИБ в АСУТП.....	14
Тема 1.4 Анализ и улучшение системы ИБ в АСУТП. Подсистемы системы защиты ПО АСУТП. Защита от разрушающих программных воздействий в АСУТП.....	18
Тема 1.5 Организация реагирования на инциденты информационной безопасности в АСУТП.....	25
3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ.....	29
4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ	30
5. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ	33
Текущая аттестация.....	33
Примерные вопросы к зачету по дисциплине	35
Заключение	36
ЛИТЕРАТУРА.....	36

ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину **«Кибербезопасность АСУТП»**.

Цель освоения дисциплины: изучение принципов построения систем защиты информации в АСУТП, способов защиты от угроз безопасности в АСУТП.

Компетенции

ПК-1. Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение

В результате освоения дисциплины обучающийся должен:

знать:

- нормативные правовые акты в области защиты информации в АСУТП;
- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации в КИИ и АСУТП;
- порядок проектирования АС в защищенном исполнении;
- национальные, межгосударственные и международные стандарты в области защиты информации АСУТП;

уметь:

- выявлять уязвимости информационно-технологических ресурсов автоматизированных систем
- определять класс защищенности автоматизированных систем и ее составных частей в КИИ, ГИС и АСУТП;

владеть:

- навыками анализа характера обрабатываемой информации и определение перечня информации, подлежащей защите в АСУТП
- разработки отчетных документов и разделов технических заданий в КИИ и АСУТП;
- разрабатывать части проектной документации на системы защиты автоматизированных систем;
- обоснования перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы в КИИ и АСУТП.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют **«Основы информационной безопасности»**, **«Технологии и методы программирования»**, **«Безопасность операционных систем»**, **«Программно-аппаратные средства защиты информации»**.

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных практических работ, мероприятий текущей

аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе, посвященном содержанию дисциплины, приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине, разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение

Типовое ПО на всех ПК

1. Операционная система Windows 10 (получаемая по программе Microsoft «Open Value Subscription»).
2. Офисное приложение MS Office Standard 2016 (получаемое по программе Microsoft «Open Value Subscription»).
3. Kaspersky Endpoint Security.
4. Google Chrome (GNU).
5. Python (GNU/Linux, macOS и Windows).
6. PascalABC.Net.
7. CODESYS.
8. Cisco Packet Tracer (GNU/Linux, macOS и Windows).
9. Oracle VirtualBox 7.1.6 и VirtualBox Extension Pack 7.1.6 for x86_64 hardware.

1. ТЕМАТИЧЕСКИЙ ПЛАН

Таблица 1 – Тематический план

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
Лекции (семестр В – 40 ч. ауд., 127,85 ч. – сам. р.)				
1.1	Специфика инцидентов ИБ в АСУТП	Тема 1.1 Специфика инцидентов ИБ в АСУТП. Протоколы АСУТП	8	25
1.2	Специфика инцидентов ИБ в АСУТП	Тема 1.2 Методы защиты ПО АСУТП	8	25
1.3	Специфика инцидентов ИБ в АСУТП	Тема 1.3 Методы и средства исследования ИБ в АСУТП	8	25
1.4	Специфика инцидентов ИБ в АСУТП	Тема 1.4 Анализ и улучшение системы ИБ в АСУТП. Подсистемы системы защиты ПО АСУТП. Защита от разрушающих программных воздействий в АСУТП	8	25
1.5	Специфика инцидентов ИБ в АСУТП	Тема 1.5 Организация реагирования на инциденты информационной безопасности в АСУТП	8	27,85
			40	127,85
Практические занятия (семестр В – 40 ч)				
1.1	Специфика инцидентов ИБ в АСУТП	Методы защиты ПО АСУТП	10	-
1.2	Специфика инцидентов ИБ в АСУТП	Основные мероприятия расследования инцидентов информационной безопасности и правонарушений в АСУТП	10	-
1.3	Специфика инцидентов ИБ в АСУТП	Организация реагирования ИБ в АСУТП	10	-

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
1.4	Специфика инцидентов ИБ в АСУТП	Методы и средства исследования ИБ в АСУТП	10	-
		Всего	40	

Курсовая работа (проект)

2.1	Специфика инцидентов ИБ в АСУТП	Контрольная точка 1. Раздел 1 (не предусмотрен)	-	-
3.1	Специфика инцидентов ИБ в АСУТП	Контрольная точка 2. Раздел 2 (не предусмотрен)	-	-
		Оформление проекта. Защита	-	-
			-	-

РЭ - 8
КА - 0,15

Рубежный (текущий) и итоговый контроль

2.1	Специфика инцидентов ИБ в АСУТП	Контроль 1	-	-
3.1	Специфика инцидентов ИБ в АСУТП	Контроль 2	-	-
		Итоговый контроль (зачет)		
		-		
			0	0
Всего			88,15	127,85

ИТОГО 216

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

Раздел 1. Методы защиты ПО

Тема 1.1 Специфика инцидентов ИБ в АСУТП. Протоколы АСУТП

Перечень изучаемых вопросов

1. Введение в АСУТП и их роль в промышленности.
2. Специфика инцидентов информационной безопасности в АСУТП.
3. Протоколы АСУТП и их уязвимости.
4. Основные угрозы и уязвимости в АСУТП.
5. Методы защиты АСУТП.
6. Нормативная база и стандарты.
7. Перспективы развития безопасности АСУТП.

Методические указания к изучению

1. Особенности АСУТП и риски киберинцидентов

Автоматизированные системы управления технологическими процессами (АСУТП) представляют собой сложные комплексы, состоящие из различных компонентов, таких как SCADA-системы (системы визуализации и управления), программируемые логические контроллеры (PLC), датчики и исполнительные устройства. Их главным отличием от классических ИТ-систем является непосредственное влияние на окружающий мир. Например, взлом SCADA-системы химического завода может привести к утечке токсичных веществ, что представляет серьезную угрозу для безопасности и здоровья людей.

Проблемы безопасности:

- Устаревшая инфраструктура: Оборудование и программное обеспечение (например, Windows XP в SCADA) часто остаются без обновлений из-за требований непрерывности производства.
- Ограниченная совместимость: Модернизация затруднена из-за длительного жизненного цикла систем (20–30 лет).
- Физические последствия: Атака на АСУТП может привести к аварии, как это произошло со Stuxnet в 2010 году, когда вирус изменил скорость вращения центрифуг в Иране, повредив оборудование.

2. Уязвимости промышленных протоколов

Протоколы АСУТП разрабатывались с целью повышения эффективности, а не безопасности, что делает их уязвимыми:

1. Modbus (используется для связи между устройствами): передача данных осуществляется в открытом виде. Отсутствие аутентификации позволяет злоумышленникам отправлять команды напрямую, что может привести к серьезным последствиям, например, открытию аварийного клапана.
2. OPC Classic (интеграция устройств) основан на устаревшем DCOM, который уязвим для перехвата данных.

3. DNP3 (энергетика):

– Существует риск подмены показаний, что может вызвать ложные данные о напряжении в сети.

4. PROFINET/Ethernet/IP (промышленный Ethernet) уязвим к DoS-атакам, которые могут парализовать сеть.

Пример атаки: в 2015 г. хакеры использовали вредоносное ПО BlackEnergy для взлома протоколов энергосистемы Украины, что привело к отключению электричества у 230 тысяч человек.

3. Основные угрозы для АСУТП

- Целевые атаки: Группы, такие как Triton, осуществляют атаки на объекты с целью саботажа. В 2017 году Triton пытался вызвать взрыв на нефтезаводе в Саудовской Аравии.

- Уязвимые интерфейсы: Веб-панели PLC часто имеют пароли по умолчанию, что делает их уязвимыми для взлома.

- Человеческий фактор: Фишинг и социальная инженерия могут использоваться для получения доступа к SCADA-системам.

- Интернет вещей (IoT): Небезопасные умные датчики становятся потенциальной точкой входа в сеть.

4. Методы защиты промышленных систем

Сегментация сетей:

- Отделение АСУТП от корпоративной сети через DMZ.

- Использование промышленных межсетевых экранов, таких как Cisco ISA-3000.

Криптография: шифрование данных в протоколах (TLS для OPC UA, VPN для удаленного доступа).

Мониторинг и обновления:

- Внедрение систем обнаружения вторжений (IDS), таких как Nozomi Networks.

- Проведение патчинга в периоды плановых остановок производства.

Обучение персонала: тренинги по кибергигиене для инженеров и операторов.

5. Нормативная база и стандарты

- IEC 62443: Международный стандарт, требующий зонирования сетей, контроля доступа и регулярного аудита.

- NIST SP 800-82: Руководство по защите промышленных систем, включая анализ угроз и настройку политик безопасности.

- ГОСТ Р 57580 (Россия): Требования к безопасности АСУТП, включая аттестацию систем по приказу ФСТЭК № 31.

6. Будущее безопасности АСУТП

- Протоколы Secure-by-Design: Modbus Secure и OPC UA с встроенным шифрованием.

- Zero Trust Architecture: Отказ от «слепого доверия» даже к внутренним компонентам.
- Искусственный интеллект: Алгоритмы машинного обучения для анализа аномалий в режиме реального времени (например, нестандартные команды в DNP3).
- Квантовая криптография: Защита от будущих угроз взлома шифрования.

Инциденты информационной безопасности в АСУТП представляют собой не просто утечку данных, а угрозу жизни людей и стабильности экономики. Основные риски связаны с устаревшими протоколами, человеческим фактором и растущей цифровизацией промышленности. Решение этих проблем требует комплексного подхода, включающего как технические меры (сегментация, криптография), так и соблюдение стандартов, и обучение персонала. Будущее безопасности АСУТП лежит в интеграции передовых технологий, таких как AI и Zero Trust, которые помогут предугадывать и нейтрализовать угрозы до их реализации.

Литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. – URL: <https://biblioclub.ru/index.php?page=book&id=467139>. – Электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. – Библиогр. в кн. - ~Б. ц. – Текст : электронный (с. 8–21).
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»; ИНФРА-М, 2013. – 416 с. (с. 23–55).
3. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения. Ч. 1. – Калининград. – 171 с. – ISBN 978-5-7481-0514-9 (с. 10–133).

Контрольные вопросы

1. Чем АСУТП принципиально отличаются от классических ИТ-систем? Приведите пример физического воздействия их уязвимостей.
2. Как длительный жизненный цикл АСУТП (20–30 лет) влияет на их безопасность?
3. Опишите инцидент с Stuxnet (2010): какие последствия он вызвал и что это говорит об угрозах для АСУТП?
4. Назовите ключевые уязвимости протокола Modbus. Какие реальные атаки возможны из-за них?
5. Как атака через протокол DNP3 может повлиять на энергосистему? Приведите пример из материала.
6. Чем опасны DoS-атаки для сетей на базе PROFINET/Ethernet/IP?

7. Почему веб-панели PLC становятся мишенью для злоумышленников?
8. Как человеческий фактор (например, фишинг) может компрометировать SCADA-системы?
9. Какие риски создает интеграция IoT-устройств в промышленные сети?

Тема 1.2 Методы защиты ПО АСУТП

Перечень изучаемых вопросов

1. ПО АСУТП и его уязвимости.
2. Основные угрозы для ПО АСУТП.
3. Методы защиты ПО АСУТП.
4. Стандарты.
5. Перспективные технологии.

Методические указания к изучению

Программное обеспечение (ПО) автоматизированных систем управления технологическими процессами (АСУТП) – это «мозг» промышленных объектов, отвечающий за управление оборудованием, сбор данных и контроль физических процессов. Однако его уязвимость к кибератакам ставит под угрозу не только производство, но и безопасность людей. В статье разбираем ключевые методы защиты ПО АСУТП и перспективные подходы к обеспечению его безопасности. ПО АСУТП включает SCADA-системы, человеко-машинные интерфейсы (HMI), прошивки программируемых логических контроллеров (PLC) и драйверы устройств. Его главные слабые места связаны со следующим:

1. Устаревшими версиями, которые не обновляются годами из-за требований непрерывности производства.
2. Открытыми интерфейсами (веб-панели, API), через которые злоумышленники могут получить доступ к системе.
3. Несовместимостью с современными средствами защиты, такими как стандартные антивирусы.

Пример: В 2021 году в SCADA-системе Citect обнаружили уязвимость CVE-2021-22204, позволяющую хакерам удалённо выполнять код через устаревшие библиотеки.

Основные угрозы для ПО АСУТП:

- Эксплуатация уязвимостей. Например, CVE-2015-5374 в Siemens SIMATIC WinCC давала злоумышленникам возможность запускать произвольные команды на серверах управления.
- Вредоносное ПО. Шифровальщики и вирусы вроде Industroyer2 (2022) атакуют энергосистемы, выводя из строя ПО управления подстанциями.
- Подмена прошивок. Атака Stuxnet продемонстрировала, как модифицированная прошивка PLC может нарушить работу центрифуг, маскируя сбой от операторов.
- Несанкционированные изменения. Внесение правок в алгоритмы управления без ведома персонала может привести к авариям.

Ключевые методы защиты:

1. Контроль доступа и аутентификация:

- Многофакторная аутентификация (MFA) для доступа к SCADA и НМІ. *Пример:* На химическом заводе внедрены смарт-карты для авторизации инженеров.

- Ролевая модель прав – разделение доступа между операторами, техниками и администраторами.

- Блокировка неиспользуемых портов (USB, Ethernet) на промышленных контроллерах.

2. Обеспечение целостности ПО:

- Цифровые подписи для проверки подлинности прошивок и обновлений.

Пример: ГОСТ Р 34.10-2012 в РФ гарантирует защиту от подмены ПО.

- Контрольные суммы – регулярная проверка целостности файлов конфигурации.

3. Защита от вредоносного кода:

- Специализированные антивирусы (Kaspersky Industrial Cybersecurity), совместимые с промышленными ОС.

- Изоляция сред – запуск критического ПО в виртуальных машинах или «песочницах».

4. Обновление и патчинг:

- Плановые окна обновлений – установка исправлений во время остановки производства.

- Тестирование в изолированной среде перед внедрением в рабочий контур.

5. Криптографическая защита:

- TLS/SSL для шифрования данных между SCADA и PLC.

- VPN-туннели (на базе IPsec) для безопасного удалённого доступа.

6. Мониторинг и аудит:

- SIEM-системы (Splunk, IBM QRadar) для анализа журналов событий и обнаружения аномалий. *Пример:* В энергокомпании внедрение Tenable.ot сократило время обнаружения атак до 15 мин.

- Регулярный аудит кода – поиск скрытых уязвимостей и «закладок».

Стандарты и нормативы:

- IEC 62443-4-1 – международный стандарт, требующий внедрения Secure SDLC (безопасный цикл разработки ПО).

- NIST SP 800-82 – рекомендации по защите промышленных систем, включая анализ угроз и настройку политик.

- Приказ ФСТЭК № 239 (РФ) – обязывает использовать сертифицированные средства защиты информации в АСУТП.

Кейсы внедрения:

1. Цифровые подписи на нефтезаводе. Внедрение ГОСТ-совместимых подписей для прошивок PLC снизило риск подмены ПО на 90 %.

2. SIEM в энергетике. Использование Splunk позволило обнаруживать попытки несанкционированного доступа к SCADA в реальном времени.

Перспективные технологии:

- Искусственный интеллект. Алгоритмы машинного обучения (Darktrace Industrial) анализируют сетевой трафик и предупреждают о подозрительных командах к PLC.

- Блокчейн. Siemens тестирует блокчейн для фиксации изменений в конфигурациях, исключая несанкционированные правки.

- Контейнеризация. Изоляция компонентов ПО в Docker-контейнерах минимизирует ущерб при взломе одного модуля.

Защита ПО АСУТП – это баланс между безопасностью и бесперебойностью производства. Устаревшая инфраструктура и растущая цифровизация требуют комплексного подхода:

А. Строгий контроль доступа и шифрование данных.

В. Следование международным стандартам (IEC 62443) и регулярный аудит.

С. Внедрение AI и блокчейна для прогнозирования угроз.

Будущее промышленной кибербезопасности – в интеграции «умных» технологий, которые не только защищают, но и учатся на угрозах, опережая злоумышленников.

Литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. – URL: <https://biblioclub.ru/index.php?page=book&id=467139>. – электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. – Библиогр. в кн. – ~Б. ц. – Текст : электронный (с. 21–30).

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»; ИНФРА-М, 2013. – 416 с. (с. 41–55).

3. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения. Ч. 1. – Калининград. – 171 с. – ISBN 978-5-7481-0514-9 (с. 100–133)

Контрольные вопросы

1. Какие компоненты входят в состав ПО АСУТП? Приведите примеры.

2. Почему обновление ПО АСУТП часто затруднено?

3. Назовите три ключевые уязвимости ПО АСУТП и поясните их причины.

4. Как атака Stuxnet повлияла на безопасность промышленных систем?

5. В чём заключается опасность подмены прошивок PLC? Приведите пример последствий.

6. Почему стандартные антивирусы не всегда подходят для защиты АСУТП? Какие решения их заменяют?

7. Какие преимущества даёт использование VPN и TLS в промышленных сетях?
8. Какие требования к безопасности ПО АСУТП содержит стандарт IEC 62443-4-1?
9. Какой вклад вносит NIST SP 800-82 в защиту промышленных систем?
10. Какие задачи решает искусственный интеллект в мониторинге безопасности АСУТП?
11. Как технология блокчейна может предотвратить несанкционированные изменения в конфигурациях PLC?

Тема 1.3 Методы и средства исследования ИБ в АСУТП

Перечень изучаемых вопросов

1. Аудит безопасности.
2. Моделирование угроз.
3. Тестирование на проникновение.
4. Анализ уязвимостей протоколов.

Методические указания к изучению

Автоматизированные системы управления технологическими процессами (АСУТП) играют важнейшую роль в критически важных инфраструктурах, таких как электростанции, нефтеперерабатывающие заводы и системы водоснабжения. Их бесперебойная работа обеспечивает стабильность и безопасность общества, а малейшая уязвимость может привести не только к финансовым потерям, но и к серьёзным экологическим катастрофам или человеческим жертвам.

Чтобы избежать подобных рисков, необходимо тщательно исследовать безопасность АСУТП на системном уровне.

Исследования информационной безопасности (ИБ) в промышленных системах направлены на решение трёх ключевых задач:

1. Выявление уязвимостей: Обнаружение недостатков в оборудовании, программном обеспечении и сетевых протоколах, которые могут быть использованы злоумышленниками для атак.
2. Оценка рисков: Оценка потенциальных кибератак, способных нарушить технологические процессы и привести к серьёзным последствиям.
3. Подтверждение соответствия стандартам: Подтверждение соответствия систем установленным стандартам, таким как IEC 62443 и NIST SP 800-82.

Пример: В 2020 году исследование SCADA-системы на химическом заводе выявило использование незащищённого протокола DNP3, что дало злоумышленникам возможность подменить данные о давлении в реакторе.

Методы исследования: от аудита до пентеста.

1. Аудит безопасности. Аудит представляет собой системный анализ компонентов АСУТП с целью поиска слабых мест. Он включает в себя несколько этапов:

А. Инвентаризация: Составление списка всех устройств (PLC, датчики, серверы) и их ролей в системе.

В. Проверка политик: Анализ настроек доступа, обновлений и резервного копирования.

С. Анализ журналов: Поиск аномалий в событиях, таких как множественные попытки входа в HMI (человеко-машинный интерфейс).

Инструменты:

1. Nessus: Сканер для обнаружения уязвимостей в сетях.

2. Wireshark: Анализатор трафика промышленных протоколов (Modbus, OPC UA).

Пример: С помощью Nessus на электростанции были обнаружены PLC с паролями по умолчанию.

2. Моделирование угроз (Threat Modeling)

Моделирование угроз помогает предсказать действия злоумышленников. Оно включает в себя три основных этапа:

1. Идентификация активов: Определение критически важных компонентов, таких как сервер управления турбиной.

2. Построение сценариев атак: Например, фишинговая атака на инженера для доступа к SCADA.

3. Оценка рисков: Ранжирование угроз по вероятности и ущербу.

Инструменты:

- Microsoft Threat Modeling Tool: Визуализация угроз через блок-схемы.

- MITRE ATT&CK for ICS: Матрица тактик атак на промышленные системы.

Кейс: при моделировании угроз для газопровода был выявлен риск перехвата данных через незашифрованный Modbus.

3. Тестирование на проникновение (Penetration Testing).

Пентест имитирует действия хакеров с целью проверки защиты. Он имеет свои особенности для АСУТП:

1. Тестирование проводится в «окна простоя», чтобы не останавливать производство.

2. Акцент на промышленные протоколы: Например, атаки на Profinet.

Инструменты:

1. Metasploit Framework: Эксплуатация уязвимостей в SCADA (например, CVE-2014-0750).

2. PLCBlaster: Проверка устойчивости контроллеров к DoS-атакам.

Пример: Пентест на нефтеперерабатывающем заводе выявил возможность удалённого выполнения кода через уязвимость в ПО WinCC.

4. Анализ уязвимостей протоколов

Промышленные протоколы, такие как Modbus и DNP3, часто не имеют встроенной защиты. Для их анализа используются следующие методы:

1. Реверс-инжиниринг: Поиск слабых мест в протоколах.

2. Эмуляция атак: Подмена данных и перехват сессий.

Инструменты:

1. Modbuspal: Эмулятор для тестирования устройств Modbus.

2. Scapy: Создание кастомных пакетов для атак на OPC UA.

Кейс: С помощью Modbuspal исследователи смоделировали атаку на насосную станцию, подменив команды управления.

Инструменты для исследования: от сканеров до цифровых двойников

1. Сканеры уязвимостей.

- Claroty – платформа для автоматического сканирования промышленных сетей. Обнаруживает устройства, анализирует конфигурации и выявляет риски.

- Tenable.ot – фокусируется на операционных технологиях (OT), проверяя соответствие стандартам NIST и IEC.

2. Системы мониторинга

- Nozomi Networks – отслеживает аномалии в трафике АСУТП (например, нестандартные команды к PLC).

- Splunk – агрегирует данные из журналов событий и визуализирует угрозы.

3. Эмуляторы и цифровые двойники

- ICS Testbed – виртуальные стенды для безопасного моделирования атак.

- CORE – создаёт цифровые копии систем управления, позволяя тестировать защиту без риска для производства.

1. Аппаратные инструменты

2. LAN Turtle – компактное устройство для скрытого перехвата трафика в промышленных сетях.

- Hak5 Rubber Ducky – эмулятор USB-устройств для тестирования физических интерфейсов.

Примеры исследований

Кейс 1: Анализ безопасности энергоподстанции. Цель: Проверить устойчивость к кибератакам. Методы:

А. Сканирование Nmap выявило открытый порт 502 (Modbus).

В. Metasploit подтвердил уязвимость PLC к несанкционированному доступу.

- Решение: Установка межсетевого экрана и обновление правил доступа.

Кейс 2: Исследование устаревшей SCADA-системы. Проблема: ПО на базе Windows XP, доступное из интернета. Действия:

А. Обнаружение через Shodan (поисковая система для IoT).

В. Эмуляция атаки с подменой данных через Modbuspal.

- Итог: Система изолирована от публичной сети, обновлена до защищённой версии.

Стандарты и руководства:

- IEC 62443 – требует регулярных аудитов, оценки рисков и зонирования сетей.

- NIST SP 800-82 – руководство по тестированию безопасности промышленных систем.

- MITRE ATT&CK for ICS – база тактик, применяемых хакерами (например, подмена данных в DNP3).

Перспективные технологии

А. Искусственный интеллект: Darktrace Industrial обнаруживает аномалии в режиме реального времени, например, необычные команды к PLC.

В. Цифровые двойники: позволяют тестировать защиту на виртуальных копиях без остановки производства.

С. Автоматизация аудита: инструменты вроде Rapid7 и Qualys проводят непрерывное сканирование уязвимостей.

Исследование ИБ в АСУТП – это не разовая проверка, а цикл из аудита, тестирования и адаптации. Ключевые вызовы:

- Работа с устаревшими системами, которые нельзя обновить.
- Минимизация влияния на производство во время пентестов.

Современные инструменты (Claroty, Nozomi Networks) и стандарты (IEC 62443) помогают систематизировать процесс, а технологии вроде ИИ и цифровых двойников открывают новые возможности. Однако успех зависит от слаженной работы ИБ-специалистов, инженеров и руководства. Будущее – за интеграцией автоматизации и прогнозной аналитики, где угрозы нейтрализуются до их реализации.

Литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. – URL: <https://biblioclub.ru/index.php?page=book&id=467139>. – Электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. – Библиогр. в кн. – ~Б. ц. – Текст : электронный (с. 21–39).

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»; ИНФРА-М, 2013. – 416 с. (с. 44–147).

3. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения. Ч. 1. – Калининград. – 171 с. – ISBN 978-5-7481-0514-9 (с. 10–133).

Контрольные вопросы

1. Какие три этапа включает аудит безопасности АСУТП?
2. Чем отличается пентест в АСУТП от классического ИТ-пентеста?
3. Как цифровые двойники помогают в исследовании безопасности?
4. Назовите два инструмента для анализа промышленных протоколов.
5. Какие риски снижает стандарт IEC 62443?

Тема 1.4 Анализ и улучшение системы ИБ в АСУТП. Подсистемы системы защиты ПО АСУТП. Защита от разрушающих программных воздействий в АСУТП

Перечень изучаемых вопросов

1. Анализ и улучшение системы ИБ в АСУТП.
2. Подсистемы системы защиты ПО АСУТП.
3. Защита от разрушающих программных воздействий.
4. Стандарты и нормативы.
5. Перспективные направления.

Методические указания к изучению

Автоматизированные системы управления технологическими процессами (АСУТП) управляют критически важными объектами – от энергосетей до химических производств. Их уязвимость к кибератакам требует не только постоянного анализа безопасности, но и внедрения многоуровневой защиты. В статье разбираем, как улучшать системы ИБ, какие подсистемы защищают ПО АСУТП и как противостоять разрушающим программным воздействиям.

1. Анализ и улучшение системы ИБ в АСУТП

1.1. Цели анализа

- Выявление слабых мест в сетях, оборудовании и ПО.
- Оценка рисков атак, способных нарушить технологические процессы.
- Проверка соответствия стандартам (IEC 62443, NIST SP 800-82).

Пример: Аудит на электростанции выявил отсутствие шифрования данных в протоколе DNP3, что позволяло злоумышленникам подменять показания счетчиков.

1.2. Методы анализа

• Аудит безопасности:

- a. Инвентаризация компонентов (PLC, серверы, датчики).
- b. Проверка настроек межсетевых экранов и политик доступа.
- c. Моделирование угроз: использование матрицы MITRE ATT&CK for ICS для прогнозирования атак.

d. Пентест: тестирование уязвимостей SCADA и PLC с помощью Metasploit Framework.

Инструменты:

- Claroty – сканирование промышленных сетей.
- Tenable.ot – анализ соответствия стандартам.

1.3. Этапы улучшения системы ИБ

• Приоритизация рисков: Ранжирование угроз по уровню опасности (например, уязвимость PLC критичнее открытого порта).

• Внедрение мер:

- A. Сегментация сетей (DMZ между ИТ и АСУТП).
- B. Обновление ПО в периоды простоя.

c. Мониторинг и адаптация: использование SIEM-систем (Splunk, IBM QRadar) для отслеживания аномалий.

- Обучение персонала: Тренинги по кибергигиене для инженеров и операторов.

Кейс: После атаки на водоканал внедрена система Nozomi Networks, что сократило время обнаружения угроз с 48 ч до 15 мин.

2. Подсистемы системы защиты ПО АСУТП

2.1. Контроль доступа

- Многофакторная аутентификация (MFA) для доступа к SCADA и HMI.
- Ролевая модель прав:
 - А. Операторы – только просмотр данных.
 - В. Инженеры – настройка параметров.
 - С. Администраторы – полный доступ.
- Блокировка неиспользуемых интерфейсов (USB, Wi-Fi).

Пример: На нефтезаводе внедрены смарт-карты для доступа к системам управления.

2.2. Обеспечение целостности ПО

- Цифровые подписи: Проверка подлинности прошивок и обновлений (ГОСТ Р 34.10-2012).
- Контрольные суммы: Регулярная проверка целостности файлов конфигурации.
- Запрет на модификацию кода без авторизации.

Инструменты:

- HashiCorp Vault – управление цифровыми сертификатами.
- Tripwire – контроль изменений в файлах.

2.3. Антивирусная защита

- Специализированные решения:

А. Kaspersky Industrial Cybersecurity – совместим с ОС реального времени (QNX, VxWorks).

В. Symantec Embedded Security – защита встроенных систем.

- Изоляция сред: Запуск ПО в виртуальных машинах или контейнерах (Docker).

Пример: Внедрение Kaspersky на заводе снизило количество инцидентов на 70 %.

2.4. Обновление и патчинг

- Плановые окна: Установка обновлений во время остановки производства.
- Тестовые среды: Проверка совместимости патчей перед внедрением.

Пример: На химическом предприятии обновление SCADA с Windows XP до Windows 10 IoT заняло 6 месяцев из-за требований к непрерывности процессов.

3. Защита от разрушающих программных воздействий

3.1. Что такое разрушающие воздействия?

- Вирусы и черви: Например, Stuxnet, изменяющий логику работы PLC.
- Шифровальщики: Industroyer2, блокирующий управление энергосистемами.

- Логические бомбы: Скрытый код, активирующийся при определенных условиях.

Пример: Атака Triton (2017) на нефтезавод в Саудовской Аравии пыталась вызвать взрыв через перепрошивку контроллеров.

3.2. Методы защиты

- Изоляция критических систем:

- А. Отключение от интернета (air-gapped сети).

- В. Использование аппаратных межсетевых экранов (Cisco ISA-3000).

- Мониторинг аномалий:

- А. Анализ поведения ПО (Darktrace Industrial).

- В. Обнаружение подозрительных команд к PLC.

- Резервное копирование: хранение копий конфигураций на автономных носителях.

3.3. Технологии противодействия

- А. Искусственный интеллект: алгоритмы машинного обучения для прогнозирования атак (анализ журналов SCADA).

- В. Блокчейн: фиксация изменений в прошивках для предотвращения подмены.

- С. Аппаратные модули безопасности (HSM): защита ключей шифрования от извлечения.

Пример: Siemens использует блокчейн для верификации прошивок PLC.

4. Стандарты и нормативы

- А. IEC 62443: требует зонирования сетей, контроля доступа и регулярного аудита.

- В. NIST SP 800-82: рекомендации по защите от разрушающих воздействий.

- С. Приказ ФСТЭК № 31: обязательная аттестация АСУТП в РФ.

- Перспективные направления

- А. Zero Trust Architecture: проверка каждого запроса, даже от доверенных устройств.

- В. Квантовая криптография: защита данных от будущих атак с использованием квантовых компьютеров.

- С. Цифровые двойники: тестирование защиты на виртуальных копиях систем.

Анализ и улучшение ИБ в АСУТП требуют системного подхода: от аудита до внедрения многоуровневых подсистем защиты. Ключевые элементы:

- А. Контроль доступа и целостности ПО – основа защиты.

- В. Борьба с разрушающими воздействиями – комбинация изоляции, мониторинга и AI.

- С. Следование стандартам – гарантия соответствия международным требованиям.

Будущее безопасности АСУТП – в интеграции инноваций: блокчейн для аудита, Zero Trust для минимизации рисков и квантовые технологии для неуязвимого шифрования. Однако успех зависит от слаженной работы технологий, процессов и людей.

Пентест (тестирование на проникновение) систем SCADA (Supervisory Control and Data Acquisition) и PLC (программируемый логический контроллер) с использованием Metasploit Framework – это процесс выявления и эксплуатации уязвимостей в автоматизированных системах управления, которые часто используются в промышленных средах, таких как энергетика, производство, водоснабжение и другие критически важные инфраструктуры. Рассмотрим этот процесс максимально подробно, включая контекст, этапы, инструменты, особенности и потенциальные риски.

Цели пентеста SCADA/PLC:

- Выявление уязвимостей: поиск слабых мест в конфигурации, программном обеспечении, сетевой инфраструктуре или протоколах.
- Оценка рисков: определение того, какие уязвимости могут быть использованы для компрометации системы, и какие последствия это может иметь (например, остановка производства, физический ущерб).
- Рекомендации по устранению: Предоставление отчета с рекомендациями по устранению выявленных проблем.
- Соблюдение нормативных требований: проверка соответствия стандартам безопасности, таким как IEC 62443, NIST 800-82 или ISO 27001.

Этапы пентеста SCADA/PLC с использованием Metasploit:

Пентест SCADA и PLC требует осторожности, поскольку атаки на промышленные системы могут привести к физическим последствиям (например, к повреждению оборудования). Обычно процесс включает следующие этапы:

Сбор информации (разведка):

- Цель: получить как можно больше данных о целевой системе без её активного воздействия.
- Методы:
 - Пассивный сбор данных: анализ открытых источников (OSINT), таких как документация, схемы сети, данные о производителе оборудования.
 - Активный сбор данных: сканирование сети с помощью таких инструментов, как Nmap, для обнаружения устройств, портов и сервисов.
 - Metasploit: Использование модулей для анализа сети, например, `auxiliary/scanner/portscan/tcp` для сканирования портов или `auxiliary/scanner/discovery/udp_sweep` для обнаружения устройств по протоколам, характерным для SCADA (например, Modbus на порту 502/TCP).
 - Протоколы SCADA/PLC: сбор информации о протоколах (Modbus, DNP3, Profibus, Ethernet/IP) и их версиях.

• Пример команды:

```
удар
msfconsole
use auxiliary/scanner/modbus/modbusclient
set RHOST <IP-адрес>
run
```

Этот модуль позволяет получать информацию о Modbus-устройствах, такую как идентификаторы и версии.

Сканирование уязвимостей:

- Цель: выявить потенциальные уязвимости в SCADA/PLC-системах, такие как устаревшее ПО, слабые пароли или открытые порты.

- Инструменты в Metasploit:

- Модули для проверки уязвимостей, например, auxiliary/scanner/scada/modbus_findunit для обнаружения устройств Modbus.

- Проверка известных уязвимостей в прошивках PLC (например, Siemens S7, Rockwell Automation).

- Использование модулей для анализа протоколов, таких как DNP3 (auxiliary/scanner/dnp3/dnp3_info).

- Пример: Проверка уязвимостей в Siemens S7 PLC:

удар

```
use auxiliary/scanner/s7/s7_identify
```

```
set RHOST <IP-адрес>
```

```
run
```

Этот модуль собирает данные о модели и версии PLC, которые можно сопоставить с базой уязвимостей (например, CVE).

Использование уязвимостей:

- Цель: попытаться использовать обнаруженные уязвимости для получения доступа или выполнения команд.

- Типичные уязвимости:

- Слабые пароли: многие SCADA-системы используют пароли по умолчанию.

- Уязвимости протоколов: например, отсутствие шифрования в Modbus или DNP3.

- Ошибки в прошивке: известные уязвимости в PLC, такие как CVE-2018-10612 для Siemens S7.

- Ошибки конфигурации: неправильная сегментация сети или открытые порты.

- Модули Metasploit:

- exploit/windows/scada/xyz (замените на конкретный модуль для целевой системы).

- Пример: Использование модуля для эксплуатации уязвимости в Modbus:

```
use auxiliary/admin/scada/modbusclient
```

```
set RHOST <IP-адрес>
```

```
set ACTION WRITE
```

```
set DATA <данныедлязаписи>
```

```
run
```

Этот модуль может изменять значения регистров в Modbus, что может привести к изменению поведения PLC.

- Полезная нагрузка: после успешной эксплуатации можно внедрить полезную нагрузку (например, Meterpreter) для дальнейшего управления системой, если это поддерживается.

Послепродажное обслуживание:

- Цель: оценить степень компрометации и собрать данные о системе.

- Действия:

- Сбор конфигурационных данных PLC (например, программной логики).
- Проверка возможности изменения параметров (например, уставок в SCADA).
- Оценка доступа к другим устройствам в сети.
- Metasploit: Использование Meterpreter или других сессий для анализа системы, сбора данных и выполнения команд.

Пример:

```
use post/windows/gather/enum_services
```

```
run
```

Этот модуль собирает информацию о сервисах в скомпрометированной системе.

Документация и отчёт:

- Цель: подготовить отчёт с описанием уязвимостей, их эксплуатации и рекомендациями.

- Содержание отчёта:

- Список обнаруженных уязвимостей с их CVE (если применимо).

- Описание сценариев эксплуатации.

- Рекомендации: обновление прошивок, смена паролей, сегментация сети, внедрение IDS/IPS.

Особенности пентеста SCADA/PLC:

- Изолированная среда: пентест лучше проводить в тестовой среде, чтобы избежать воздействия на реальные процессы.

- Специфические протоколы: необходимы знания протоколов SCADA/PLC (Modbus, DNP3, OPC, S7comm), поскольку они отличаются от стандартных IT-протоколов.

- Ограниченная поддержка в Metasploit: хотя в Metasploit есть модули для SCADA, их может быть недостаточно для всех систем, и потребуется использование дополнительных инструментов (например, Wireshark, PLCinject, Snap7).

Примеры модулей Metasploit для SCADA/PLC:

- Modbus:

- вспомогательный/сканер/modbus/modbusclient: для чтения/записи данных в устройства Modbus.

- вспомогательный/административный/scada/modbus-клиент: для выполнения административных функций.

- DNP3:

- вспомогательное/сканирование/dnp3/dnp3_info: Сбор информации об устройствах DNP3.

- Siemens S7:

- вспомогательный/сканер/s7/s7_identify: Идентификация Siemens PLC.

- Общие модули:

- вспомогательный/сканер/сканирование портов/tcp: Сканирование портов.

- exploit/multi/handler: Управление полезной нагрузкой.

Риски и ограничения:

- Физический ущерб: неправильное изменение параметров PLC может привести к сбоям в работе оборудования.
 - Юридические аспекты: Пентест должен проводиться только с письменного разрешения владельца системы.
 - Ограниченная документация: многие SCADA/PLC-системы имеют закрытую документацию, что затрудняет тестирование.
 - Ложные срабатывания: некоторые действия могут быть ошибочно приняты системой мониторинга за реальную атаку.
- Рекомендации по безопасности SCADA/ПЛК:
- Сегментация сети: изолировать SCADA/PLC от корпоративных сетей и Интернета.
 - Шифрование: использовать VPN или зашифрованные протоколы для передачи данных.
 - Обновления: регулярно обновляйте прошивку и ПО.
 - Мониторинг: Внедрить системы обнаружения вторжений (IDS) для промышленных сетей.
 - Аутентификация: используйте сложные пароли и многофакторную аутентификацию.

Пример сценария пентеста:

• Ситуация: Пентест SCADA-системы на электростанции с PLC Siemens S7.

Шаги:

- Сканирование сети с помощью Nmap для обнаружения устройств (порт 102 для S7comm).
- Использование вспомогательного/сканера/s7/s7_identify для определения модели и версии PLC.
- Поиск уязвимостей в базе данных CVE (например, CVE-2018-10612).
- Попытка эксплуатации уязвимости с использованием соответствующего модуля Metasploit.
- Изменение параметров PLC (например, чтение/запись регистров) для демонстрации уязвимости.

• Подготовка отчёта с рекомендациями по устранению неполадок.

Помимо Metasploit, для пентеста SCADA/PLC можно использовать:

- Wireshark: анализ трафика промышленных протоколов.
- PLCscan: Сканирование PLC-устройств.
- Snap7: Инструмент для работы с Siemens S7.
- Nmap NSE-скрипты: специальные скрипты для SCADA-протоколов.

Пентест SCADA и PLC с использованием Metasploit Framework — это сложный процесс, требующий глубоких знаний промышленных систем, протоколов и инструментов. Metasploit предоставляет широкие возможности для сканирования, эксплуатации и анализа, но его использование должно сопровождаться осторожностью и соблюдением этических норм. Для успешного тестирования важно учитывать специфику промышленных систем, проводить тести-

рование в контролируемой среде и предоставлять чёткие рекомендации по устранению уязвимостей.

Литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. – URL: <https://biblioclub.ru/index.php?page=book&id=467139>. – Электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. – Библиогр. в кн. – ~Б. ц. – Текст : электронный (с. 21–60).

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»; ИНФРА-М, 2013. – 416 с. (гл. 9).

3. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения. Ч. 1. – Калининград. – 171 с. – ISBN 978-5-7481-0514-9 (с. 100–133).

Контрольные вопросы

1. Какие этапы включает улучшение системы ИБ в АСУТП?
2. Как цифровые подписи защищают целостность ПО?
3. Назовите два примера разрушающих программных воздействий на АСУТП.
4. Какие технологии помогают прогнозировать кибератаки на промышленные системы?
5. Почему стандарт IEC 62443 важен для защиты АСУТП?

1.5 Организация реагирования на инциденты информационной безопасности в АСУТП

Перечень изучаемых вопросов

1. Введение в инциденты ИБ в АСУТП: специфика и последствия.
2. Этапы реагирования на инциденты.
3. Инструменты и технологии для обнаружения и анализа.
4. Роль команды CSIRT (Computer Security Incident Response Team).
5. Примеры реальных инцидентов и их устранение.
6. Стандарты и нормативные требования.
7. Перспективы: автоматизация и искусственный интеллект в реагировании.

Методические указания к изучению

Автоматизированные системы управления технологическими процессами (АСУТП) контролируют энергосети, нефтепроводы, химические производства. Их компрометация может привести не только к утечке данных, но и к физиче-

ским авариям. Реагирование на инциденты ИБ в таких системах требует особого подхода – скорости, точности и учёта специфики промышленной инфраструктуры.

1. Введение в инциденты ИБ в АСУТП: специфика и последствия

Инцидент ИБ в АСУТП – это событие, которое ставит под угрозу конфиденциальность, целостность или доступность системы. Однако, в отличие от ИТ-инцидентов, здесь последствия могут быть катастрофическими:

- Физические аварии: Взрыв на заводе из-за подмены данных в SCADA.
- Экологический ущерб: Утечка нефти из-за взлома системы управления трубопроводом.
- Остановка производства: Простой предприятия на дни или недели.

Пример: В 2021 г. хакеры атаковали систему управления водоканалом во Флориде, пытаясь изменить уровень химикатов в воде. Инцидент удалось предотвратить благодаря оперативному обнаружению.

2. Этапы реагирования на инциденты.

2.1. Подготовка:

- Создание плана реагирования: Чёткие инструкции для команды.
 - Обучение персонала: Тренинги для инженеров и операторов.
 - Резервное копирование: Хранение копий конфигураций PLC и SCADA.
- Инструменты: Документация по стандарту NIST SP 800-61.

2.2. Обнаружение:

- Мониторинг аномалий:
 - а. Нестандартные команды к PLC (например, остановка насоса без причины).
 - в. Подозрительный трафик в промышленных протоколах (Modbus, OPC UA).
- Источники данных: журналы событий SCADA, сигналы от IDS (например, Nozomi Networks).

Пример: Система Claroty обнаружила несанкционированный доступ к контроллеру Siemens S7-1200 через порт 102.

2.3. Анализ:

- Определение масштаба: какие компоненты затронуты (PLC, серверы, датчики)?
- Классификация инцидента:
 - а. Утечка данных.
 - в. Подмена команд управления.
 - с. Внедрение вредоносного ПО (типа Triton).

Инструменты:

- а. Wireshark – анализ сетевого трафика.
- в. Autopsy – исследование заражённых систем на наличие артефактов.

2.4. Сдерживание

- Изоляция заражённых узлов: Отключение PLC от сети.
- Блокировка атакующего: Обновление правил межсетевого экрана (Cisco Firepower).

Пример: При атаке на энергоподстанцию инженеры вручную перевели управление в локальный режим, отключив удалённый доступ.

2.5. Ликвидация

- Удаление вредоносного кода: Очистка SCADA-серверов.
- Восстановление прошивок: Перезапись PLC с резервной копии.

Инструменты: Kaspersky Industrial Cybersecurity для очистки встроенных систем.

2.6. Восстановление

- Проверка целостности: Контрольные суммы конфигураций.
- Постепенный ввод в эксплуатацию: Запуск системы поэтапно для контроля.

2.7. Пост-анализ

- Разбор полётов: Причины инцидента, ошибки в защите.
- Обновление политик: Например, запрет использования паролей по умолчанию.

3. Инструменты и технологии

- SIEM-системы (Splunk, IBM QRadar): Агрегация данных из SCADA и PLC.
- Специализированные IDS (Nozomi Networks, Darktrace): Обнаружение аномалий в промышленных протоколах.
- Песочницы (Cuckoo Sandbox): Анализ подозрительных файлов до их попадания в сеть АСУТП.

Кейс: Энергетическая компания внедрила Tenable.ot, что сократило время реакции на инциденты с 8 ч до 30 мин.

4. Роль команды CSIRT

- Состав команды:

А. Инженеры АСУТП – понимание технологических процессов.

В. Специалисты по кибербезопасности – анализ угроз.

С. Юристы – работа с регуляторами.

- Обязанности:

А. Круглосуточный мониторинг.

В. Координация с персоналом предприятия.

Пример: На химическом заводе CSIRT отработал инцидент с шифровальщиком за 4 часа, восстановив данные из резервных копий.

5. Примеры реальных инцидентов

- Атака на Colonial Pipeline (2021):

А. Последствия: Остановка нефтепровода, дефицит топлива в США.

В. Реагирование: Компания заплатила выкуп, но восстановила системы из бэкапов.

- Инцидент с Triton (2017):

А. Действия хакеров: Внедрение вредоносного ПО для перепрошивки контроллеров.

В. Реакция: Отключение заражённых узлов и аудит всех PLC.

6. Стандарты и нормативные требования

- IEC 62443-2-1: Требования к процессам реагирования на инциденты.

- NIST SP 800-82: Руководство по созданию CSIRT для промышленных систем.

- Приказ ФСТЭК № 239 (РФ): Обязанности по расследованию инцидентов.

7. Перспективы развития

А. Автоматизация реагирования: использование SOAR-платформ (Palo Alto Cortex XSOAR) для автоматического блокирования атак.

В. Искусственный интеллект: прогнозирование инцидентов на основе анализа журналов.

С. Цифровые двойники: тестирование сценариев реагирования на виртуальных копиях АСУТП.

Реагирование на инциденты в АСУТП требует слаженной работы людей, процессов и технологий. Ключевые факторы успеха:

А. Скорость: Минимизация времени между обнаружением и ликвидацией.

В. Экспертиза: Понимание как киберугроз, так и технологических процессов.

С. Проактивность: Регулярные учения и обновление планов реагирования.

Будущее – за интеграцией AI и автоматизации, но даже самые продвинутые инструменты не заменят подготовленных специалистов. Безопасность АСУТП начинается с осознания, что каждый инцидент – это урок, который делает систему устойчивее.

Литература

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. – URL: <https://biblioclub.ru/index.php?page=book&id=467139>. – Электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. – Библиогр. в кн. – ~Б. ц. – Текст : электронный (с. 39–65).

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»; ИНФРА-М, 2013. – 416 с. (гл. 9, 15).

3. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения. Ч. 1. – Калининград. – 171 с. – ISBN 978-5-7481-0514-9 (с. 10–133).

Контрольные вопросы

1. Чем инциденты ИБ в АСУТП отличаются от инцидентов в классических ИТ-системах?

2. Назовите три этапа реагирования на инциденты и кратко опишите каждый.

3. Какие инструменты используются для анализа сетевого трафика в АСУТП?
4. Какую роль играет команда CSIRT в управлении инцидентами?
5. Приведите пример реального инцидента в АСУТП и опишите, как он был устранён.
6. Какие стандарты регулируют организацию реагирования на инциденты в промышленных системах?
7. Почему пост-анализ инцидента важен для улучшения безопасности?
5. Как технология цифровых двойников помогает в отработке сценариев реагирования?
6. Какие риски возникают при использовании автоматизации в реагировании на инциденты?
7. Чем вредоносное ПО для АСУТП (например, Triton) отличается от обычных вирусов?
8. Как блокируются атакующие при сдерживании инцидента?
9. Какие этические проблемы могут возникнуть при расследовании инцидентов в АСУТП?

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Практические занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины. Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Рекомендации к подготовке

1. Изучение лекционного материала и конспектов:

- перед практическими занятиями необходимо проработать соответствующие разделы лекционного материала;
- рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом практического занятия.

2. Проработка учебной литературы:

- используйте основные учебники и методические пособия, рекомендованные преподавателем;
- для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Решение типовых задач:

- проработать примеры и типовые задачи из учебных материалов, методических указаний;

– выполните задачи, предложенные преподавателем для самостоятельной работы, что обеспечит лучшее понимание методов и подходов к решению задач.

4. Подготовка вопросов:

– составьте список вопросов по материалу, вызвавшему затруднения;
– обсуждение этих вопросов на лабораторном занятии поможет устранить пробелы в знаниях.

5. Вопросы для самоконтроля:

– перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

Тематический план практических занятий приводится в разделе «Тематический план».

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкреплённая самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста);
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники;
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы;
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам;
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов;
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) – важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к зачету;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный

характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);

- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудиовидеозаписей):

- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции;

подготовка рефератов, докладов;

- работа с компьютерными программами.

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений;
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;

- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудиовидеотехники и компьютерных расчетных программ, и электронных практикумов;

- подготовка курсовых проектов и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Методические указания по курсовой работе – не предусмотрено.

Методические указания по выполнению расчетно-графической работы – не предусмотрено.

5. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Текущая аттестация

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная либо балльно-рейтинговая. Выбрана традиционная зачетно-экзаменационная методика оценивания знаний. Предусматриваются: зачет.

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: контроль самостоятельной работы по темам дисциплины, контроль выполнения практических работ.

К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100–балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полной знаний и системным взглядом на изучаемый объект

Система оценок Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	между собой)			
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задачи данные	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

Завершающим этапом изучения дисциплины является итоговая аттестация, представляющая собой зачет.

Допуск к итоговой аттестации возможен при:

- наличии всех выполненных, сданных (проверенных, защищенных) лабораторных работах, наличии отчётов по ним;
- наличии показателей приемлемого уровня освоения материалов курса: более 50 % посещений от общего числа требуемых по учебному плану.

Примерные вопросы к зачету по дисциплине

Вопросы к зачету

1. Проанализируйте инцидент со Stuxnet: какие уязвимости АСУТП он эксплуатировал?
2. Как длительный жизненный цикл оборудования влияет на безопасность АСУТП?
3. Сравните уязвимости протоколов Modbus и OPC Classic.
4. Проанализируйте архитектуру защиты ПО АСУТП по стандарту IEC 62443-4-1.
5. Почему стандартные антивирусы часто неприменимы в АСУТП?
6. Как организовать безопасное обновление ПО на непрерывном производстве?
7. Сравните эффективность VPN и TLS для защиты промышленных протоколов.
8. Какие перспективы у использования ИИ для защиты АСУТП?
9. Как цифровые двойники помогают в тестировании защиты АСУТП?
10. Проанализируйте эффективность инструментария Nozomi Networks для мониторинга.
11. Какие риски возникают при пентестинге работающего промышленного оборудования?
12. Как применить матрицу MITRE ATT&CK for ICS для оценки защищенности завода?
13. Разработайте план перехода от устаревшей SCADA к защищенному решению.
14. Как реализовать принцип нулевого доверия (Zero Trust) в АСУТП?
15. Проанализируйте кейс с Triton: какие уроки по защите можно извлечь?
16. Какие методы защиты наиболее эффективны против подмены прошивок PLC?
17. Разработайте пошаговый план реагирования на атаку шифровальщика в АСУТП.
18. Как организовать работу CSIRT на нефтеперерабатывающем заводе?
19. Проанализируйте инцидент с Colonial Pipeline: какие ошибки были допущены?

20. Какие SIEM-системы наиболее эффективны для АСУТП и почему?
21. Как автоматизировать реагирование на инциденты с помощью SOAR?
22. Сравните угрозы для АСУТП в энергетике и химической промышленности.
23. Как интегрировать новые технологии защиты (ИИ, блокчейн) в устаревшие АСУТП?
24. Предложите меры защиты для изолированной (air-gapped) системы управления.
25. Оцените перспективы применения квантовой криптографии в АСУТП.
26. Как цифровые двойники могут улучшить безопасность промышленных систем?
27. Возможности и риски использования 5G в АСУТП.
28. Как ИИ может улучшить обнаружение аномалий в промышленных протоколах?
29. Сравните требования NIST SP 800-82 и приказа ФСТЭК №239.
30. Как организовать аттестацию АСУТП по российским стандартам?
31. Какие проблемы возникают при согласовании международных стандартов ИБ?

ЗАКЛЮЧЕНИЕ

Правильная организация учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

ЛИТЕРАТУРА

Основные источники

1. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. – URL: <https://biblioclub.ru/index.php?page=book&id=467139>. – Электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация. – Библиогр. в кн. – ~Б. ц. – Текст : электронный.
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»; ИНФРА-М, 2013. – 416 с.

3. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения. Ч. 1. – Калининград. – 171 с. – ISBN 978-5-7481-0514-9.

Дополнительные источники

4. Васильева, И. Н. Расследование инцидентов информационной безопасности: учеб. пособие / И. Н. Васильева. – Санкт-Петербург: Изд-во СПбГЭУ, 2019. – 113 с

5. Национальная безопасность: учебник / В. И. Абрамов, М. А. Газимагомедов, К. К. Гасанов [и др.]; под ред. К. К. Гасанова, Н. Д. Эриашвили, О. А. Мироновой. – 3-е изд., перераб. и доп. – Москва: ЮнитиДана, 2023. – 288 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=700171> (дата обращения: 05.06.2024). – ISBN 978-5-238-03639-7. – Текст : электронный.

6. Информационная безопасность распределенных информационных систем: метод. указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Текст : непосредственный. Ч. 1 / сост. В. В. Подтопельный. – 2020. – 61 с.

7. Подтопельный, В. В. Информационная безопасность распределенных информационных систем. Ч. 2. Методические указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / В.В. Подтопельный (3 авт. л.).

8. Подтопельный, В. В. Комплексное обеспечение информационной безопасности автоматизированных систем. Ч. 1. Методические указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / В. В. Подтопельный, А. А. Бабаева. – Калининград: Изд-во БГАРФ, 2021. – 53 с. (3 авт. л.).

Учебно-методические пособия, нормативная литература

9. «Доктрина информационной безопасности Российской Федерации» (утв. Указом Президентом РФ 05.12.2016 № 646 (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

10. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

11. Федеральный закон от 28.12.2010 N 390-ФЗ «О безопасности» (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

12. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

13. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

14. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

15. Федеральный закон от 15.11.2010 N 299-ФЗ «О внесении изменений в статью 5 Закона Российской Федерации «О государственной тайне» (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

16. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера» (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

17. «ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

18. «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373-ст) (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

19. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. Решением Гостехкомиссии России от 30.03.1992) (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

20. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Решением Гостехкомиссии России 30.03.1992) (в действующей редакции). – Доступ из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

21. ГОСТ Р ИСО/МЭК ТО 18044-2007.

Локальный электронный методический материал

Владислав Владимирович Подтопельный

КИБЕРБЕЗОПАСНОСТЬ АСУТП

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,2. Печ. л. 2,4.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1