МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор НОЦ «Институт
непрерывного образования»
_____ Е.В. Мошкина
«__» марта 2024 г.

ДОПОЛНИТЕТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Информационная безопасность систем промышленной автоматизации»

Красноярск 2024

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Аннотация программы

Программа повышения квалификации направлена на знакомство слушателей с современной проблематикой информационной безопасности и ее аспектами, актуальными в масштабе предприятий и организаций, приобретение и углубление знаний в области методологии информационной безопасности, правового, организационного и технического обеспечения, в т.ч. особенностями защиты информации в компьютерной и сетевой среде, защиты речевой информации, защиты персональных данных, коммерческой и служебной тайны.

Информационная безопасность обеспечивает защиту программ и данных от несанкционированного доступа посредством программных и программно-аппаратных средств информационной безопасности.

Специалисты в этой сфере работы должны уметь обеспечивать необходимый уровень защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости.

Перечисление этих знаний и практических навыков говорит о высокой сложности получения такой профессии, не говоря уже о том, что специалисты в этой сфере должны проходить регулярную дополнительную подготовку, так как изменения в этой области очень часто имеют очень сложную конструкцию.

1.2. Цель программы

Цель программы повышения квалификации — формирование профессиональных компетенций в сфере комплексного обеспечения информационной безопасности на промышленных предприятиях, освоение механизмов обеспечения информационной безопасности систем промышленной автоматизации, изучение практических решений управления информационной безопасностью с учетом современных тенденций в постоянно развивающейся области защиты информации.

1.3. Компетенции (трудовые функции) в соответствии с Профессиональным стандартом (формирование новых или совершенствование имеющихся) и/или национальной рамкой квалификаций РФ.

В соответствии с профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н), можно выделить следующие трудовые функции, на формирование и совершенствование которых направлена программа повышения квалификации (6-ой уровень квалификации):

А/01.5 Обслуживание программно-аппаратных средств защиты информации в операционных системах.

А/02.5 Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях.

А/03.5 Обслуживание средств защиты информации прикладного и системного программного обеспечения.

В/01.6 Администрирование подсистем защиты информации в операционных системах.

1.4. Планируемые результаты обучения

Слушатели в результате освоения программы повышения квалификации «Информационная безопасность систем промышленной автоматизации» смогут:

РО1. Проводить оценку эффективности применения программно-аппаратных средств защиты информации в системах и сетях объектов промышленной автоматизации.

РО2. Проводить обслуживание системы защиты информации автоматизированных систем, настройку подсистем защиты информации в операционных системах.

РО3. Участвовать в оценке и обработке рисков информационной безопасности технологических процессов.

РО4. Планировать построение и поддержание эффективности программно-аппаратных средств защиты информации АСУ ТП.

РО5. Проводить анализ применения технологии безопасной разработки программных продуктов АСУ ТП.

РО6. Применять требования регуляторов при подборе, внедрении и обслуживании средств защиты информации в системах промышленной автоматизации и применении компенсирующих мер.

1.5. Категория слушателей

Лица, получающие высшее образование по очной (очно-заочной) форме, лица, освоившие образовательную программу бакалавриата в объеме не менее первого курса (бакалавры 2-го курса), образовательную программу специалитета — не менее первого курса (специалисты 3-го курса), владеющие навыками разработки компьютерных программ.

1.6. Требования к уровню подготовки поступающего на обучение

Программа повышения квалификации рассчитана на всех студентов, обучающихся на инженерных специальностях, заинтересованных граждан, имеющих высшее образование по профилю деятельности. Необходимо свободное владение компьютером, базовыми интернет-технологиями (системы искусственного интеллекта, поиск, электронная почта).

1.7. Продолжительность обучения: 72 часа, из них 36 контактных, 36 часов — самостоятельная практическая работа.

1.8. Форма обучения: очно-заочная с применением электронного обучения и дистанционных образовательных технологий.

1.9. Требования к материально-техническому обеспечению, необходимому для реализации дополнительной профессиональной программы повышения квалификации (требования к аудитории, компьютерному классу, программному обеспечению).

Обучение по программе повышения квалификации реализуется на платформе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/). При проведении лекций, практических занятий, самостоятельной работы слушателей используется следующее оборудование: компьютер с наушниками или аудиоколонками, микрофоном и веб-камерой, высокоскоростное подключение к Интернет (не менее 5 Мбит/с).

Программное обеспечение (обновленное до последней версии): браузер Yandex, системы SberJazz, Яндекс-Телемост, сервис видеоконференций СФУ https://i.sfu-kras.ru/conference/.

1.10. Особенности (принципы) построения дополнительной профессиональной программы профессиональной переподготовки.

Особенности построения программы повышения квалификации «Информационная безопасность систем промышленной автоматизации» в рамках Инженерного образовательного центра:

– все занятия, кроме самостоятельных работ, проводятся дистанционно в синхронном и асинхронном режиме;

– в основу проектирования программы положен компетентностный подход;

– учебные задания требуют практического применения знаний и умений, полученных в ходе изучения лекционного и практического материала;

– требуется выполнение итоговых работ по реальному заданию;

– применяется использование информационных и коммуникационных технологий, в том числе систем технической поддержки процесса обучения, обеспечивающих комфортные условия для обучающихся, преподавателей;

– используются электронные образовательные ресурсы (дистанционное, электронное, комбинированное обучение и пр.).

В поддержку дополнительной профессиональной программы профессиональной переподготовки должен используется электронный курс на платформе: https://e.sfu-kras.ru/course/.

1.11. Документ об образовании: удостоверение о прохождении курса повышения квалификации установленного образца.

УЧЕБНЫЙ ПЛАН
программы повышения квалификации
«Информационная безопасность систем промышленной автоматизации»

Форма обучения – очно-заочная с использованием электронного обучения и дистанционных образовательных технологий.
Срок обучения – 72 часа.

№ п/п	Наименование модулей (дисциплин)	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы		СРС, ч	Формы контроля
				Лекции	Практические и семинарские занятия		
1.	Модуль 1. Информационная безопасность технологических автоматизированных систем	34	16	6	10	18	Тестирование
2.	Модуль 2. Основы безопасной разработки АСУ ТП	34	16	6	10	18	Тестирование
	Итоговый контроль	4	2			2	Зачет
	Итого	**72**	**34**			**38**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
программы повышения квалификации
«Информационная безопасность систем промышленной автоматизации»

Категория слушателей: лица, имеющие/получающие высшее образование.
Срок обучения: 4 недели.
Форма обучения: очно-заочная с использованием электронного обучения и дистанционных образовательных технологий.
Режим занятий: 3-4 часа в день.

№ п/п	Наименование модулей (курсов)	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы		СРС, ч	Результаты обучения
				Лекции	Практ. и семинарские занятия		
1	**Модуль 1. Информационная безопасность технологических автоматизированных систем**	**34**	**16**	**6**	**10**	**18**	**РО1–РО3, РО6**
1.1	Методологические подходы в области информационной безопасности АСУ ТП	10	4	2	2	6	РО1–РО3, РО6
1.2	Методы и средства обеспечения информационной безопасности в промышленных системах, построение модели угроз	12	6	2	4	6	РО1–РО3, РО6
1.3	Особенности применения средств защиты информации в системах промышленной автоматизации	12	6	2	4	6	РО1–РО3, РО6
2	**Модуль 2. Основы безопасной разработки АСУ ТП**	**34**	**16**	**6**	**10**	**18**	**РО1, РО4–РО6**
2.1	Жизненный цикл безопасной разработки программного обеспечения, требования стандартов	10	6	2	4	6	РО1, РО4–РО6
2.2	Обеспечение необходимого уровня доверия в системах промышленной автоматизации	12	6	2	4	6	РО1, РО4–РО6
2.3	Регламент безопасной разработки и средства обеспечения безопасности	12	4	2	2	6	РО1, РО4–РО6
	Итоговая аттестация	**4**	**2**			**2**	**РО1–РО6**
	Итого	**72**	**34**			**38**	

II. ОСНОВНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. План учебной деятельности

Результаты обучения	Учебные действия/ формы текущего контроля	Используемые ресурсы/ инструменты/технологии
РО1. Проводить оценку эффективности комплекса технических и организационных мер обеспечения информационной безопасности на объектах промышленной автоматизации	Лекции и практические задания. Выполнение задания по разработке плана мер обеспечения информационной безопасности, подбор средств защиты. Тесты.	Материалы электронного курса и задания для выполнения в системе электронного обучения СФУ «е-Курсы». Видеоконференции.
РО2. Проводить проверки работоспособности системы защиты информации автоматизированной системы	Лекции и практические задания. Разработка политики информационной безопасности, инструкций по выполнению мер защиты объектов АСУ ТП. Тесты	Материалы электронного курса и задания для выполнения в системе электронного обучения СФУ «е-Курсы». Видеоконференции.
РО3. Участвовать в оценке и обработке рисков информационной безопасности технологических процессов	Лекции и практические задания. Выполнение задания по формированию экспертной комиссии по оценке рисков информационной безопасности. Тесты.	Материалы электронного курса и задания для выполнения в системе электронного обучения СФУ «е-Курсы». Видеоконференции.
РО4. Планировать построение и поддержание системы информационной безопасности АСУ ТП на требуемом уровне.	Лекции и практические задания. Выполнение задания по разработке мер обеспечения информационной безопасности, подбор средств защиты объектов АСУ ТП. Тесты.	Материалы электронного курса и задания для выполнения в системе электронного обучения СФУ «е-Курсы». Видеоконференции.
РО5. Проводить анализ применения технологии безопасной разработки программных продуктов АСУ ТП	Лекции и практические задания. Выполнение задания по разработке регламента безопасной разработки. Тесты.	+ Материалы электронного курса и задания для выполнения в системе электронного обучения СФУ «е-Курсы». Видеоконференции.
РО6. Применять требования регуляторов при подборе технических средств защиты информации в системах промышленной автоматизации и применении компенсирующих мер	Лекции и практические задания. Выполнение задания по разработке плана мер обеспечения информационной безопасности, подбор средств защиты. Тесты.	Материалы электронного курса и задания для выполнения в системе электронного обучения СФУ «е-Курсы». Видеоконференции.

2.2. Виды и содержание самостоятельной работы

Для обеспечения программы разработаны учебно-методические материалы по всем модулям и темам программы.

Слушатели обеспечены доступом к учебно-методическим материалам в электронном виде — для изучения теоретического материала и обеспечения самостоятельной работы, а также учебно-методическими на электронных курсах для проведения практических занятий.

Для изучения теоретического материала, нормативных актов и организации самостоятельной работы слушателям предоставляется доступ в системе электронного обучения СФУ (http://e.sfu-kras.ru) к курсу, включающему в себя презентации занятий, материалы для самостоятельного изучения, иллюстрирующие видеоматериалы, ссылки на законодательные акты по теме программы. Доступ в систему электронного обучения (логин, пароль) предусматривает возможность изучения и скачивания необходимых материалов для выполнения практических заданий, возможность скачивания презентационных, учебно-методических и нормативных материалов, осуществления обратной связи и контактов с преподавателями программы.

III. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

3.1. Учебно-методическое обеспечение, в т.ч. электронные ресурсы в корпоративной сети СФУ и сети Интернет

1. Информационная безопасность открытых систем: [учеб. для вузов]: [в 2 т.] / С.В. Запечников [и др.]. – Т. 2: Средства защиты в сетях. – М.: Горячая линия -Телеком, 2008. – 558 с.

2. Калинина Н.А. Методы и средства защиты информации: учеб. пособие для специальности 230105 очн., очн. сокр. и заочн. форм обучения / Н.А. Калинина; [отв. ред. Г.А. Доррер]. – Красноярск: СибГТУ, 2009. – 196 с.

3. Партыка, Т. Л., Попов И. И. Информационная безопасность: учебное пособие / Т. Л. Партыка, И. И. Попов / Москва Форум НИЦ ИНФРА-М, 2014. – 5-е изд., перераб. и доп. – 432с.

4. Прохорова О.В. Информационная безопасность и защита информации / О.В. Прохорова / СГАСУ (Самарский госуд. арх.-строит. ун-т), 2014. – 114 с.

5. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: [учеб. пособие для вузов] / П.Б. Хорев. – М.: Академия, 2008. – 256 с.

6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства: [учеб. пособие для вузов] / В.Ф. Шаньгин. – М.: ДМК Пресс, 2008. – 544 с.

7. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: [учеб. пособие для вузов] / В.Ф. Шаньгин. – М.: ФОРУМИНФРА-М, 2010. – 592 с.

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Формы аттестации, оценочные материалы, методические материалы

Программа предусматривает проведение текущей и итоговой аттестации. Текущая аттестация слушателей проводится по каждой теме лекционных материалов на основе выполнения практических заданий в электронном обучающем курсе.

Методические материалы, необходимые для выполнения текущих заданий, представлены в соответствующих элементах электронного обучающего курса и включают описание задания, методические рекомендации по его выполнению, критерии оценивания.

Контроль результатов обучения по программе включает в себя:

– промежуточную аттестацию в рамках практических занятий — презентация проектов, анализа конкретных ситуаций, рассматриваемых в рамках проведения киберучений и диагностических упражнений;

– итоговую аттестацию — итоговое тестирование.

Примеры тестовых заданий в итоговом тесте.

1. Отметьте какими техническими мерами стоит дополнить существующую систему ИБ АСУ ТП:
    a. Приобрести систему контроля доступа к узлам АСУ ТП.
    b. Установить на вход в помещения с АСУ ТП вход по биометрическим параметрам.
    c. Установить двухфакторную аутентификацию на для удалённых пользователей.
    d. Усилить антивирусную защиту.
    e. Применить всё перечисленное.
    f. Обновить модель угроз и определить необходимые средства из перечисленных (правильный ответ).
2. Что такое «событие информационной безопасности»?
    a. Выявленное состояние системы, услуги или сети, указывающее на возможное нарушение политики обеспечения ИБ (правильный ответ).
    b. Выявленное состояние системы, услуги или сети, указывающее на сбой мер обеспечения ИБ (правильный ответ).
    c. Выявленная неизвестная ситуация, которая может иметь отношение к вопросам безопасности (правильный ответ).
    d. Выявленное состояние системы, услуги или сети, указывающее на наличие сбоев в работе сетевых сервисов.

3. Безопасное программное обеспечение — это:
   a. ПО, разработанное с использованием совокупности мер, направленных на предотвращение и устранение уязвимостей программы (правильный ответ).
   b. ПО, разработанное с использованием средств для анализа исходного кода, для анализа готовых проектов, при использовании средств поиска уязвимостей.
   c. ПО, разработанное командой специально обученных программистов и специалистов по информационной безопасности.
   d. ПО, разработанное для использования на объектах информатизации, где должна быть обеспечена защита информации.

4.2. Требования и содержание итоговой аттестации

Основанием для аттестации является выполнение итогового online тестирования в рамках электронного обучающего курса в системе электронного обучения СФУ.

Для проведения итоговой аттестации разработан банк тестовых заданий по всем темам программы повышения квалификации:

1. Информационная безопасность технологических автоматизированных систем:

– Методологические подходы в области информационной безопасности АСУ ТП.

– Методы и средства обеспечения информационной безопасности в промышленных системах, построение модели угроз.

– Особенности применения средств защиты информации в системах промышленной автоматизации.

2. Основы безопасной разработки АСУ ТП:

– Жизненный цикл безопасной разработки программного обеспечения, требования стандартов.

– Обеспечение необходимого уровня доверия в системах промышленной автоматизации.

– Регламент безопасной разработки и средства обеспечения безопасности.

Банк тестовых заданий составляет 100 тестовых вопросов.

Итоговый тест в электронной системе обучения СФУ включает в себя 25 вопросов по двум модулям программы.

Тестирование ограничено по времени, результаты демонстрируются слушателям непосредственно сразу после окончания итоговой аттестации.

Для получения оценки «зачтено» слушателю необходимо набрать не менее 40 % верных ответов в итоговом тесте.

Программу составил:

Канд. физ.-мат. наук, доцент кафедры информационной безопасности Института космических и информационных технологий СФУ  В.Б. Туговиков

Руководитель программы:

Канд. физ.-мат. наук, доцент кафедры информационной безопасности Института космических и информационных технологий СФУ  В.Б. Туговиков