



ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ В ОБЛАСТИ ИБ

СИБИРСКАЯ АКАДЕМИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SAIB.BIZ

INFO@SAIB.BIZ

+7 (383) 255 32 55

Проблематика

Развитие технологий и внедрение новых средств обработки информации требуют не только уверенного владения компьютером, но и знаний правил работы с электронной почтой, носителями информации, Интернетом и пр.

Однако не следует забывать, что вместе с развитием сетевых технологий уровень доступа к ресурсам растет, как и количество разнообразных атак на эти ресурсы.

В настоящее время практически в каждой организации в работе используется огромный объем информации, представляющей значительную ценность для компании в целом и для сотрудников в частности.

В современных условиях, наряду со знанием и исполнением трудовых обязанностей, от работника **требуется знание специфических вопросов, связанных с обеспечением ИБ**, что обусловлено не только нормативными документами компании, но и элементарными требованиями безопасности и необходимостью сохранения конфиденциальной информации в тайне.

К сожалению, значительное число инцидентов ИБ, связанных прежде всего с утечками конфиденциальной информации, вирусными заражениями или уничтожением/искажением информации, **происходит по вине работников**. Таким образом, уровень осведомленности пользователей в сфере информационной безопасности является одним из основных факторов, которые существенно влияют на состояние ИБ в компании.

ВНЕШНИЕ ФАКТОРЫ

Рост киберугроз

- Автоматизация
- Нейросети
- Процессный подход

Рост рисков

- Переход в онлайн
- Электронные деньги
- Электронное имущество
- Конфиденциальная информация

ВНУТРЕННИЕ ФАКТОРЫ

Отсутствие процессного подхода к обучению и оценке ИБ

- Отсутствие методики оценки и проверки зрелости процессов ИБ
- Уровень готовности сотрудников к угрозам
- Корректный запуск процессов

Нехватка экспертизы в направлении

- Нет профессиональных квалифицированных сотрудников
- Контроль и проверка деятельности сотрудников
- Правильный подход к обучению сотрудников

Зависимость от человеческого фактора

- Корректность настройки системы безопасности
- Реагирование системы на инциденты
- Слабая осведомленность в тематиках социальной инженерии

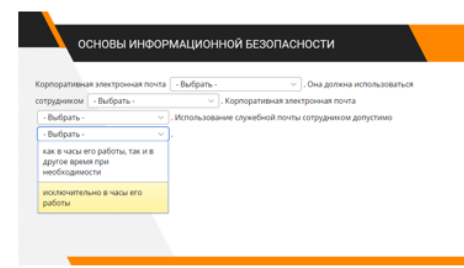
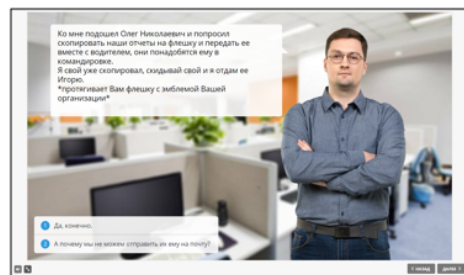
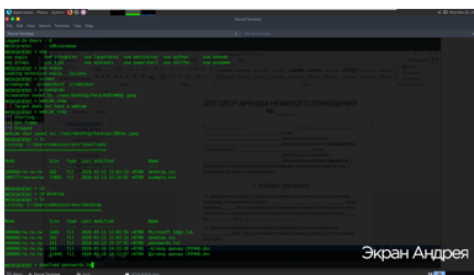
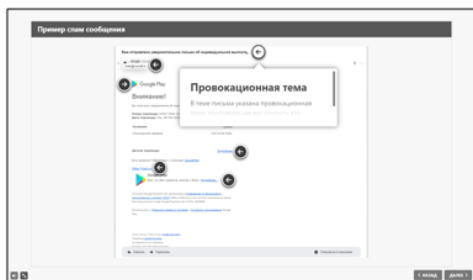
Учебные курсы

С целью сохранения информационных ресурсов Вашей компании в безопасности «Сибирская академия информационной безопасности» предлагает Вам повышать осведомленность сотрудников в сфере ИБ комплексно.

Под повышением осведомленности работников компании в области ИБ понимается целенаправленный, организованный, планомерно и систематически осуществляемый процесс повышения уровня знаний работников и формирования необходимых навыков в области ИБ.

Учебные курсы являются основой построения процесса повышения осведомленности сотрудников в вопросах информационной безопасности на предприятии и помогают донести до пользователей и специалистов текущие положения по информационной безопасности в Компании и осветить основные угрозы ИБ и методы защиты от них.

Наши учебные курсы содержат актуальную теорию, интерактивные области, промежуточные тестирования, диалоговые тренажеры, фото- и видеоконтент. Комплексное применение различных форм и методов обучения обеспечивает наиболее эффективное усвоение информации.



СИБИРСКАЯ АКАДЕМИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SAIB.BIZ

INFO@SAIB.BIZ

+7 (383) 255 32 55

Разработка курсов

Также мы предлагаем разработку учебных курсов «под ключ» по Вашему запросу – только интересующие Вас темы в необходимом объеме и форме с нужными методическими акцентами и оригинальной развлекающей составляющей, разработанные специально для Вас профессиональными консультантами по ИБ.

Чтобы наши учебные материалы в полной мере удовлетворяли необходимые Заказчику требования, при создании учебных курсов по информационной безопасности мы руководствуемся регламентами ИБ конкретной организации, а также учитываем фирменный стиль компаний.

Мы гарантируем **персональный подход** к каждому, ведь только тесное взаимодействие наших редакторов и аналитиков со службами ИБ Заказчика приводит в результате к **качественному учебному материалу**, который будет действительно обучать пользователей организации, а не создавать лишь видимость обучения.

Каждый созданный курс мы передаем в формате SCORM.

SCORM – это международный стандарт для создания электронного курса. Почти любая система дистанционного обучения (СДО) поддерживает данный стандарт (Blackboard, Moodle, OLAT, tools.hrm.ru от WebSoft, ShareKnowledge от Competentum, Mirapolis LMS, Webtutor). Материалы, которые Вы загрузите в систему обучения, откроются с любого компьютера через любой Интернет-браузер.


ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Программное обеспечение – системные и прикладные программы, установленные на корпоративные сервера и персональные компьютеры сотрудников. ПО, предоставленное сотруднику для выполнения должностных обязанностей, находится в его зоне ответственности.

Сотрудник обязан контролировать ПО от неправомерного использования посторонними лицами.

Сотрудник запрещается:

- устанавливать и запускать ПО, не входящее в утвержденный перечень ПО, используемого на рабочих станциях и серверах;
- эксплуатировать ошибки ПО рабочих станций.



НАЧИНАЯ РАБОТУ С СИСТЕМОЙ

В локальной вычислительной сети Банка используется несколько паролей:

- Для входа в систему Windows;
- Для работы в АБС;
- Для других специализированных программ и электронной почты.


Требования к паролям:

- Не может содержать частично (или полностью) имя из учетной записи пользователя;
- Должен содержать не менее шести символов;
- Должен содержать символы минимум из трех следующих категорий:
 - Английские прописные буквы (от А до Z);
 - Английские строчные буквы (от а до z);
 - Цифры от 0 до 9;
 - Неалфавитные символы (например, \$, #, %)

ВАЖНО ЗНАТЬ!

Персональные данные относятся к сведениям конфиденциального характера, т.е. Вы не можете совершать с ними любые действия без письменного согласия пользователя.

Если вы заметили, что сотрудник производит манипуляции с чужими персональными данными, необходимо обратиться к сотруднику безопасности информации.



Модуль 3 Управление инцидентами информационной безопасности

Способность и разноеобразие среды деятельности современного бизнеса предопределяет наличие рисков возникновения инцидентов ИБ.



SOCIAL ENGINEERING IN PRACTICE


Having prepared everything necessary, Andrew goes for lunch to the same cafe as the employees of the hacked company.

Noticing a group of people at the table, Andrew headed towards them.

- "Hi guys", Andrew greeted them.
- "Good afternoon", reluctantly answered him four young people seated together at one table.
- Hey listen, I eat here every day and yesterday before lunch I found a flash drive on the table.

* Andrew gives them a USB flash drive with the company logo of the organization he is attacking on it and continues his conversation *

- "Yesterday I decided not to give the flash drive to the administrator of this cafe because, you do realize by yourself, most likely, she will take it and won't be looking for the owner. I guess you are from this company, so I ask you to give the flash drive to its owner."



ПОНЯТИЕ ИНТЕРНЕТ

Интернет – всемирная система объединенных компьютерных сетей. Интернет образует всемирную (единую) информационную среду.

Интернет предоставляет пользователям **информационные и коммуникационные возможности**:

- обеспечивает доступ к информационным ресурсам сети и возможность размещения собственной информации в сети;
- позволяет осуществлять обмен информацией в отключенном режиме и в режиме реального времени.

Каждый компьютер, подключаемый к международной сети Интернет, имеет свой уникальный адрес, который виден другим участникам глобальной сети. Это является главной опасностью при подключении к всемирной информационной среде.



Почему это важно?

Учебные курсы, содержащие теоретические и практические материалы – это именно то, с чего следует начать повышать уровень осведомленности сотрудников в сфере информационной безопасности.

Повышение осведомленности персонала - это один из важнейших этапов внедрения системы обеспечения ИБ, который направлен на обучение персонала и поддержание его знаний в актуальном состоянии.

Конечной целью обучения является снижение ущерба и потерь от угроз, связанных с человеческим фактором при работе с информационными ресурсами компании.

Чтобы ознакомиться с полным перечнем предоставляемых нами услуг более детально, мы предлагаем Вам записаться на **бесплатный вебинар** по комплексному повышению осведомленности в сфере информационной безопасности, на котором мы расскажем об инновационном подходе к обучению и продемонстрируем наши решения в работе.

Контактная информация:

info@saib.biz

+7 (383) 255 32 55

КУРСЫ ППО

ЭКСПЕРТНЫЕ КУРСЫ

БРЕНДИРОВАНИЕ

РАЗРАБОТКА

ВХОДНЫЕ ТЕСТИРОВАНИЯ



ФИШИНГ

ПЕНТЕСТ

КИБЕРУЧЕНИЯ

АВТОМАТИЗАЦИЯ

ИНТЕГРАЦИЯ

СИБИРСКАЯ АКАДЕМИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SAIB.BIZ

INFO@SAIB.BIZ

+7 (383) 255 32 55