АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

Б1.В.09 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Код и наименование направления подготовки: 38.04.02 Менеджмент
Направленность (профиль): «Управление софтверными компаниями»
Квалификация (степень) выпускника: магистр
Форма обучения: очная

Цель освоения дисциплины: сформировать способность оценивать возможность изменения действующей корпоративной стратегии, программы организационного развития и изменений

План курса:

Тема 1. Теоретические основы информационной безопасности.

Предмет и задачи теории защиты информации. Базовые термины и определения. Классификация угроз безопасности. Интерпретация угрозы атаки. Понятие надежности безопасности, параметры и характеристики безопасности. Классификация угроз уязвимостей и уровней защиты (защищенности). Объекты защиты и объекты моделирования.

Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Тема 2. Обеспечение информационной безопасности в условиях глобализации информационного пространства

Информационная безопасность в информационном обществе. Современное информационное противоборство и обеспечение информационной безопасности.

Информационная безопасность в системе национальной безопасности Российской Федерации. Базовые принципы обеспечения информационной безопасности. Правовое регулирование информационной безопасности в системе российского информационного права. Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации. Правовые средства обеспечения безопасности информации. Организационное обеспечение информационной безопасности Российской Федерации.

Тема 3. Правовые режимы обеспечения безопасности информации ограниченного доступа

Ограничение доступа к информации в целях защиты интересов личности, общества и государства. Правовые режимы тайн в системе организационного и правового обеспечение безопасности информации ограниченного доступа. Правовой режим защиты государственной тайны. Правовой режим коммерческой тайны. Правовой режим обеспечения безопасности персональных данных. Актуальные вопросы режима служебной тайны.

Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию. Правовые проблемы обеспечения информационной безопасности в сети Интернет

Тема 4. Юридическая ответственность за правонарушения в информационной сфере.

Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты и объекты правоотношений в области обеспечения информационной безопасности. Преступность в информационной сфере как

угроза информационной безопасности при формировании информационного общества в условиях глобализации. Проблемы уголовно-правовой ответственности за информационные преступления. Проблемы международного сотрудничества и зарубежный опыт противодействия преступлениям в информационной сфере

Тема 5. Проектирование систем защиты информации

Основополагающие методы и абстрактные модели контроля доступа. Абстрактные модели контроля доступа к защищенным режимам обработки информации. Модели и методы ролевого и сессионного контроля доступа. Вопросы идентификации ролей и сессий. Задачи построения системы защиты информации. Альтернативные методы защиты информации.

Стадии и задачи проектирования. Определение функциональных задач системы защиты информации. Определение требований к качеству разработки и технического сопровождения системы защиты информации. Экономическое обоснование проектных решений. Оценка производительности системы защиты информации. Эксплуатационное проектирование системы защиты информации.

Тема 6. Анализ и управление рисками в сфере информационной безопасности

Управление рисками. Модель безопасности с полным перекрытием. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001. Методики построения систем защиты информации. Методики и программные продукты для оценки рисков. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель».

Формы текущего контроля и промежуточной аттестации:

В ходе реализации дисциплины Б1.В.09 «Информационная безопасность» текущий контроль успеваемости проводится в устной и письменной формах. Используются следующие методы текущего контроля успеваемости обучающихся:

№	Наименование тем и/или разделов	Методы текущего контроля успеваемости
Тема 1	Теоретические основы информационной безопасности	О
Тема 2	Обеспечение информационной безопасности в условиях глобализации информационного пространства	К
Тема 3	Правовые режимы обеспечения безопасности информации ограниченного доступа	ПО
Тема 4	Юридическая ответственность за правонарушения в информационной сфере	Э
Тема 5	Проектирование систем защиты информации	Т
Тема 6	Анализ и управление рисками в сфере информационной безопасности	Т

Условные обозначения: опрос(Э), кейс(К), письменный опрос(ПО), эссе(Э), тестирование(Т), зачет (За)

Основная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 c. — 978-5-9963-0237-6. — Режим доступа: http://www.iprbookshop.ru/52182.html
2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. —

Режим доступа: http://www.iprbookshop.ru/52209.html
3. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 c. — 978-89838-487-6. — Режим доступа: http://www.iprbookshop.ru/6991.html