

**УТВЕРЖДАЮ**

Директор филиала ФГБОУ ВПО «БГУЭП»

в г. Усть-Илимске

  
А.В. Бандурист

« 06 » Сентябрь 2014 г.

### Аннотация рабочей программы дисциплины

#### Б1.В.ДВ.9.2 Информационная безопасность

<b>Цели освоения дисциплины</b>	<ul style="list-style-type: none"><li>– формирование знаний и умений, связанных с организацией информационной безопасности, планированием, подготовкой и реализацией процесса информационной безопасности,</li><li>– освоение различных технологий обеспечения информационной безопасности,</li><li>– применение форм и методов обучения с учетом возрастных особенностей и специфики обучения.</li></ul>
<b>Место дисциплины в учебном плане и трудоемкость в зачетных единицах</b>	<p>Данная дисциплина относится к вариативной части дисциплин по выбору. Дисциплина дает базовую основу для понимания, анализа и оценки основных проблем, связанных с обеспечением ИБ предприятия и защитой информации, а также разработкой, внедрением и сопровождением средств информационной защиты, и ее изучение базируется на полученных студентами знаниях при освоении предшествующих дисциплин: «Математика», «Информатика».</p> <p>Общая трудоемкость дисциплины составляет 3 зачетные единицы.</p>
<b>Формируемые компетенции</b>	ОПК-1, ОПК-2.
<b>Знания, умения и навыки, формируемые в результате освоения дисциплины</b>	<p>В результате освоения дисциплины студент должен:</p> <p>Знать: современную научную парадигму информационной безопасности; организационно-правовые основы защиты информационных ресурсов предприятия; теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи; модели, стратегии систем и технологических основ комплексного обеспечения информационной безопасности; вопросы правового и организационного обеспечения информационной безопасности; концепцию информационной безопасности; содержание основных понятий обеспечения информационной безопасности; источники угроз безопасности информации; методы оценки уязвимости информации; методы создания, организации и обеспечения функционирования систем комплексной защиты информации; методы пресечения разглашения конфиденциальной информации; виды и признаки компьютерных преступле-</p>

	<p>ний, особенности основных следственных действий при расследовании указанных преступлений.</p> <p>Уметь: решать вопросы в сфере обеспечения информационной безопасности; применять практические навыки и способности по осуществлению мероприятий по обеспечению информационной безопасности; использовать методы и средства защиты данных; выполнять анализ способов нарушений информационной безопасности; отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.</p> <p>Владеть: основными понятиями безопасности информации; средствами обеспечения информационной безопасностью.</p>
<b>Содержание дисциплины</b>	<p>Раздел 1. Обеспечение информационной безопасности: содержание и структура понятия. Раздел 2. Стандарты и спецификации в области информационной безопасности. Раздел 3. Комплексная система защиты информации. Раздел 4. Процедурный уровень информационной безопасности. Раздел 5. Административный уровень информационной безопасности.</p>
<b>Виды учебной работы</b>	<p>Лекции, семинарские занятия, практические работы, самостоятельная работа.</p>
<b>Характеристика образовательных технологий, информационных, программных и иных средств обучения, с указанием доли аудиторных занятий, проводимых в интерактивных формах</b>	<p>Лекции с проблемным изложением, лекции-дискуссии, написание рефератов.</p> <p>Интернет-ресурсы: <a href="http://www.securitylab.ru/">http://www.securitylab.ru/</a>.  <a href="http://www.anti-malware.ru/">http://www.anti-malware.ru/</a>. <a href="http://ib.sa-sec.org/">http://ib.sa-sec.org/</a>.  <a href="http://infosecurity.report.ru/">http://infosecurity.report.ru/</a>. <a href="http://bib.pps.ru/">http://bib.pps.ru/</a>.  <a href="http://www.inattack.ru/">http://www.inattack.ru/</a>. <a href="https://securityvulns.ru/">https://securityvulns.ru/</a>.  <a href="https://attack-on-web.net/showthread.php?p=39978">https://attack-on-web.net/showthread.php?p=39978</a>.  <a href="https://www.pgpru.com/">https://www.pgpru.com/</a>. <a href="https://nordrus.info/security/">https://nordrus.info/security/</a>.  <a href="https://tuib.ru/">https://tuib.ru/</a>. <a href="http://habrahabr.ru/blogs/infosecurity/">http://habrahabr.ru/blogs/infosecurity/</a>.</p> <p>Доля аудиторных занятий, проводимых в интерактивных формах, составляет 50%.</p>
<b>Формы текущего контроля успеваемости студентов</b>	<p>Рефераты, контрольные работы, тестирование.</p>
<b>Виды и формы промежуточной аттестации</b>	<p>Экзамен в устной форме или в форме тестирования.</p>