МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_____»_____2017 г.

ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Методические рекомендации по подготовке к самостоятельным работам для направления подготовки магистратуры 10.04.01 «Информационная безопасность» для студентов всех форм обучения

Курск 2017

УДК 621.(076.1)

Составители: А. А. Гребеньков, А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Организационное и правовое обеспечение информационной безопасности [Текст]: методические рекомендации подготовке к практическим занятиям для направления подготовки магистратуры 10.04.01 «Информационная безопасность» для студентов всех форм обучения / Юго-Западный гос. ун-т; сост.: А. А. Гребеньков, А.Г. Спеваков. Курск, 2017. 45 с.: прилож. 1.

Излагаются методические рекомендации по подготовке к практическим занятиям по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Даются рекомендации относительно общих принципов подготовки к самостоятельным работам, правила оформления рефератов, приводятся планы занятий, литература, тезисы ответа, темы рефератов и контрольные вопросы. Методические рекомендации соответствуют требованиям программы дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности».

Предназначены для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность» всех форм обучения

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл. печ. л. . Уч.-изд. л. . Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.

Самостоятельная работа №1 – **Принципы, силы, средства и условия организационной защиты информации.**

Важным является рассмотрение информационной безопасности как неотъемлемой составной части национальной безопасности Российской Федерации. Это ясно определяется Концепцией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской федерации от 10 января 2000 года и Доктриной информационной безопасности Российской Федерации от 9 сентября 2000 года. Здесь система национальных интересов России определяется совокупностью основных интересов личности, общества и государства. При этом на современном этапе интересы личности состоят в реальном обеспечении конституционных прав и свобод, личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии.

Интересы общества включают в себя упрочение демократии, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение России.

Интересы государства состоят в защите конституционного строя, суверенитета и территориальной целостности России, в установлении политической, экономической и социальной стабильности, в безусловном исполнении законов и поддержании правопорядка, в развитии международного сотрудничества на основе партнерства.

Концепция определяет национальные интересы России в информационной сфере. Национальные интересы России обусловливают необходимость сосредоточения усилий общества и государства на решение определенных задач. Такими являются: соблюдение конституционных прав и свобод граждан в области получения информации и обмена ею, защита национальных духовных ценностей, пропаганда национального, культурного наследия, норм морали и общественной нравственности, обеспечение права граждан на получение достоверной информации, развитие современных телекоммуникационных технологий. Планомерная деятельность государства по реализации этих задач позволит Российской Федерации стать одним из центров мирового развития в XXI веке. В то же время недопустимо

использование информации для манипулирования массовым сознанием. Необходима защита государственного информационного ресурса от утечки важной политической, экономической, научно-технической и военной информации.

В соответствии с данной Концепцией важнейшими задачами обеспечения информационной безопасности являются:

– установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

– совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

– разработка соответствующей нормативной правовой базы и координация, при ведущей роли Федерального агентства правительственной связи и информации при Президенте Российской Федерации, деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;

– развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

– защита государственного информационного ресурса, и, прежде всего в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Вопросы:

1. Раскрыть содержание задач обеспечения информационной безопасности страны.
2. Дать определение понятия информационной безопасности России.
3. Назовите задачи и назначение подзаконных нормативных правовых актов, регулирующих процессы защиты информации в отраслях и предприятиях различных форм собственности.

4. Определите правовые основы защиты различных видов информации.

Самостоятельная работа №2 -

Порядок засекречивания и рассекречивания сведений, документов и продукции

Закон РФ «О государственной тайне» регулирует отношения, возникающие в связи с отношением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.

В качестве базы для Закона «О государственной тайне» был избран Закон РФ «О безопасности» от 28 декабря 2010 г., впервые введенный в действие Постановлением Верховного Совета РФ 05.03.1992 г.

Порядок засекречивания сведений и их носителей определяет 3 раздел закона «О государственной тайне». В ней представлены:

→ принципы засекречивания;

→ сведения, не подлежащие засекречиванию;

→ степени секретности сведений и грифы секретности носителей этих сведений;

→ порядок отнесения сведений к государственной тайне;

→ ограничение прав собственности предприятий, учреждений, организаций и граждан РФ на информацию в связи с ее засекречиванием;

→ порядок засекречивания сведений и их носителей;

→ реквизиты носителей сведений, составляющих государственную тайну.

В четвертом разделе дан порядок рассекречивания сведений и их носителей, включающий:

→ порядок рассекречивания сведений;

→ порядок рассекречивания носителей сведений, составляющих государственную тайну;

→ порядок исполнения запросов граждан, предприятий, учреждений, организаций и органов государственной власти РФ о рассекречивании сведений.

Вопросы:

1. Порядок разработки перечня сведений, подлежащих засекречиванию.
2. Процедура предварительного засекречивания.

3. Порядок рассекречивания.

4. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.

Самостоятельная работа №3 -

Особенности системы организационной защиты информации, составляющей государственную тайну

СВЕДЕНИЯ, ОТНОСИМЫЕ К ГТ			
Сведения в военной области	*Сведения в области экономики науки, техники*	*Сведения В области внешней политики и экономики*	*Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности*

Классификация сведений, относимых к государственной тайне

Важной особенностью настоящей концепции защиты информации является переход от принципа «интегральной защиты» информации к «дифференциальной защите», обеспечивающей разумную достаточность в соответствии с запросами государственных структур и отдельных граждан. При этом необходимо отметить, что все законодательные акты имеют содержательную различную направленность по защите информации в органах государственной власти и частных лиц. Задача создания стройной законодательной системы, одновременно удовлетворяющей всем изложенным требованиям комплексной защиты информации, оказывается сложной задачей и на сегодняшний день не имеет адекватных решений.

Определяющим принципом конституционных информационных отношений является принцип свободы и ограничения информации. Принцип свободы в более широком контексте является центральным принципом всего конституционного регулирования. Конституция официально подтверждает международно-признанное право граждан на информацию. Статьи Конституции РФ раскрывают содержание этого права. Пункт 4 ст. 29 гласит: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

Вопросы:

1. В каком порядке информация относится к Государственной тайне?
2. Какими законами и актами раскрывается право граждан на информацию?

В каком разделе закона «О государственной тайне» определен порядок распоряжения сведениями, составляющими государственную тайну?

Самостоятельная работа №4 -

Допуск и доступ к конфиденциальной информации и документам, составляющим коммерческую тайну

Основным условием обеспечения сохранности коммерческой тайны является персональная ответственность должностных лиц фирмы всех уровней и других ее работников, которым предоставлен доступ к коммерческой тайне, за соблюдение режима конфиденциальности, установленного упомянутыми организационно-методическими документами (доводятся до сведения указанных лиц под расписку). Должностные лица и сотрудники организации (фирмы) в случае разглашения ими информации, составляющей предмет защиты конфиденциальных интересов, нарушения порядка обращения с материальными носителями конфиденциальной информации или средствами информатизации и связи, используемыми для обработки и передачи указанной информации, а также в случае несанкционированного ознакомления с объектами интеллектуальной собственности посторонних лиц, несут дисциплинарную и материальную ответственность.

Обязанность возмещения убытков от указанных неправомерных действий виновным лицом возникает в случае, если условия о соблюдении конфиденциальности включены в трудовой договор (контракт) с работником или гражданско-правовой договор с контрагентом (п. 2 ст.139 Гражданского кодекса). В случае деловых контактов фирмы с иностранными партнерами взаимные обязательства сторон о неразглашении информации, которая определяется ими как конфиденциальная, срок действия этих обязательств, санкции за их невыполнение и другие аспекты отражаются в рамках документа о намерениях сторон.

Передача конфиденциальной информации и объектов интеллектуальной собственности другим физическим и юридическим лицам производится на основе лицензионного договора.

Вопросы:

1. Допуск к государственной тайне.
2. Степень секретности.
3. Гриф секретности.
4. Доступ к сведениям, составляющих государственную тайну.

Самостоятельная работа №5 -

Организация внутриобъектового и пропускного режимов на предприятиях

При организации и обеспечении пропускного и внутриобъектового режимов особое внимание следует уделять правилам внутреннего распорядка и работе с кадрами. При приеме на работу администрация обязана проинструктировать работника по правилам безопасности и сохранности информации с оформлением письменного договора. Работники обязаны строго соблюдать требования по обеспечению безопасности и защиты информации, соблюдать установленный порядок работы, хранения, передачи материальных ценностей и документов.

Важным препятствием являются контрольно-пропускные пункты, которые устанавливаются для осуществления пропуска людей и транспорта, выноса (вноса) или вывоза (ввоза) материальных ценностей и документов. Такие пункты могут быть контрольно-проходными. Они в свою очередь подразделяются на внешние (доступ на территорию) и внутренние (доступ в здание, помещение). Контрольно-проездные пункты оборудуются проездными воротами, площадками или эстакадами для досмотра транспорта, шлагбаумами или вспомогательными воротами, смотровыми вышками и смотровыми ямами, постовыми будками и пр.

Особое значение следует уделять системе охранной сигнализации, которая размещается на путях возможного движения правонарушителя, таким образом, чтобы любое нарушение охраняемой зоны вызывало срабатывание датчиков. Например, периметры объектов, охраняемых ведомственной военизированной охраной, оборудуются техническими средствами различного принципа действия не менее, чем в два рубежа.

Первый рубеж — оборудуется по козырьку основного ограждения. Второй рубеж оборудуется в запретной зоне.

Пропускной и внутриобъектовый режим представляют собой совокупность организационно-правовых правил, которыми регламентируется порядок входа (выхода), въезда (выезда) на объект (территорию) и отдельные участки. Режим устанавливается с целью организации контроля и проверки лиц, транспортных

средств и материальных ценностей в момент пере-сечения ими границы поста, а также фиксации следов видимых и скрытых попыток возможного хищения материальных ценностей с охраняемых объектов предприятия, его закрытых территорий и территорий ограниченного доступа.

Основанием выдачи пропуска для прохода на охраняемый объект является заявка на пропуск. Выдача разового пропуска позволяет однократно в течение рабочего времени находиться на определенной территории. Временный пропуск предусмотрен для лиц, которые работают по контракту, и постоянный пропуск – для лиц, которые состоят в штате. Как правило, утраченные пропуска объявляются недействительными. Допуск на охраняемый объект в выходные, праздничные дни и в ночное время осуществляется по спискам, утвержденным руководством объекта.

Вопросы:

1. Понятие пропускного режима.
2. Цели и задачи пропускного режима.
3. Организация пропускного режима
4. Организация и обеспечение работ по защите информации. Установление мер контроля и ответственности.

Самостоятельная работа №6 -

Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. Защита информации при публикаторской и рекламной деятельности

Нарушения, связанные с проведением служебных совещаний:

– проведение совещаний в не аттестованных помещениях без соответствующего разрешения руководителя предприятия или его заместителей;

– допуск на совещание лиц, не имеющих отношения к обсуждаемым вопросам и участие которых не вызывается служебной необходимостью;

– несоблюдение очередности рассмотрения вопросов конфиденциального характера;

– несоблюдение требований внутриобъектового режима при проведении совещаний;

– фотографирование, демонстрация конфиденциальных изделий, фильмов без согласования с СБ;

– звукозапись выступлений участников совещания на носителе, не учтенном в СБ;

– направление тетрадей (записей) секретного характера в учреждения, которых эти сведения непосредственно не касаются;

– недостаточное знание работниками, участвующими в приеме командированных лиц, требований инструкции о порядке приема командированных лиц (об этом заявили около 45% опрошенных лиц).

Вопросы:

1. Порядок подготовки помещения к совещанию.
2. Условия и порядок взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями.
3. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ.

4. Передача сведений, составляющих государственную тайну, другим государствам или международным организациям.

5. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений.

Самостоятельная работа №7 -

Организация аналитической работы по предупреждению утечки конфиденциальной информации.

Интересы юридических лиц, действующих на разных условиях в рыночных отношениях, в значительной степени отличаются от прежней монопольной позиции государства, прежде всего тем, что в основе этих интересов лежит острая необходимость обезопасить себя (свой коммерческий интерес) от риска и угроз. Важным является то, что в этом случае государство само начинает выступать в качестве субъекта, также требующего защиты от риска, угроз, охраны коммерческой тайны, защиты от шпионажа (в том числе и промышленного). Если же эти угрозы реализуются, то субъекту причиняется ущерб в виде прямых финансовых потерь или упущенной выгоды. Несколько последних лет позволили набрать статистику по фактам преступлений в финансовой сфере. Анализ наиболее крупных из них, связанных с хищением валютных и денежных средств во Внешэкономбанке по поддельным финансовым документам дает основания полагать, что статистика финансовых компьютерных преступлений не будет отличаться от аналогичной статистики в западных странах. Близкими оказываются и побудительные мотивы этих преступлений. Таким образом, к настоящему времени сформировались направления, требующие законодательной поддержки:

→ защита персональных данных;

→ борьба с компьютерной преступностью, в первую очередь в финансовой сфере;

→ защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;

→ защита государственных секретов;

→ создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;

→ обеспечение безопасности АСУ потенциально опасных производств;

→ страхование информации и информационных систем;

→ сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;

→ организация взаимодействия в сфере защиты данных со странами – членами СНГ и другими государствами.

Вопросы:

1. Факторы применения различных форм стимулирования ответственного отношения сотрудников к обеспечению информационной безопасности фирмы.
2. Предпосылки и условия применения различных форм стимулирования ответственного отношения сотрудников к обеспечению информационной безопасности фирмы
3. Место и роль психологического климата в коллективе при проведении воспитательной работы в коллективе фирмы.
4. Реквизиты носителей сведений, составляющих государственную тайну.

Самостоятельная работа №8 -

Направления и методы работы с персоналом, обладающим конфиденциальной информацией

Усилия руководства предприятия должны быть сосредоточены на следующих основных направлениях работы с сотрудниками, допущенными к конфиденциальной информации:

– изучение морально-деловых качеств сотрудников предприятия;

– повышение ответственности сотрудников всех категорий за сохранение в тайне доверенных по службе сведений конфиденциального характера;

– проведение профилактической работы по предупреждению (исключению) утечки конфиденциальной информации путем ее разглашения;

– повышение уровня теоретических знаний и практических навыков сотрудников в вопросах защиты конфиденциальной информации;

– создание и поддержание устойчивого морально-психологического климата в коллективе предприятия;

– создание и применение системы стимулирования труда сотрудников, допущенных к конфиденциальной информации.

В число основных методов проверки и оценки соответствия кандидата предъявляемым требованиям входят:

– изучение материалов личного дела, анкетных, автобиографических и других персональных данных, резюме и иных документов кандидата;

– личная беседа с кандидатом должностных лиц предприятия (работников кадрового органа);

– проведение тестирования.

Вопросы:

1. Перечислите методы работы с персоналом.
2. Какие направления работы с персоналом наиболее важны?
3. Цели и задачи работы с персоналом, обладающим конфиденциальной информацией.
4. Стадии работы с персоналом, обладающим конфиденциальной информацией.