**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ЮУрГГПУ»)**
**ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ**

**Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам**

# Формирование компетентности сотрудников в области информационной безопасности в образовательной организации

**Магистерская диссертация**
**по направлению: 44.04.04 Профессиональное обучение (по отраслям)**
**Направленность (профиль): Управление информационной безопасностью в профессиональном образовании**
**Форма обучения заочная**

Проверка на объем заимствований:
_____% авторского текста

Работа рекомендована к защите
«__» _____ 2021 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил(а):
Студент(ка) группы ЗФ-309-210-2-1
Цаплин Виталий Михайлович

Научный руководитель:
Уварина Наталья Викторовна, д.п.н.,
профессор

**Челябинск**
**2021**

**МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ**
**РОССИЙСКОЙ ФЕДЕРАЦИИ**
**Федеральное государственное бюджетное образовательное учреждение**
**высшего образования**
**«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-**
**ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(ФГБОУ ВО «ЮУрГГПУ»)**
**ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ**

**Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам**

# Разработка рекомендаций системы защиты персональных данных в профессиональной образовательной организации

**Магистерская диссертация**
**по направлению: 44.04.04 Профессиональное обучение (по отраслям)**
**Направленность (профиль): Управление информационной безопасностью в профессиональном образовании**
**Форма обучения заочная**

Проверка на объем заимствований:
77 % авторского текста

Работа рекомендована к защите
«18» 01 2021г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнила:
Студентка группы ЗФ-309-210-2-1
Мельник Нина Юрьевна

Научный руководитель:
Уварина Наталья Викторовна, д.п.н,
профессор

**Челябинск**
**2021**

Оглавление

# ВВЕДЕНИЕ

XXI век – это век высоких компьютерных технологий. С быстрым течением времени информация стала неотъемлемой частью процесса обучения. В современном обществе образование является одной из самых значимых сфер человеческой деятельности. По общему признанию, ведущую роль в происходящих изменениях играют стремительно развивающиеся новые информационные технологии, изменившие за последние десятилетия весь цивилизованный мир.

Одной из самых важных неотъемлемых характеристик информационных ресурсов многие исследователи считают их принципиальную уязвимость от различного рода угроз информационной безопасности, поэтому тесная зависимость экономического потенциала и конкурентоспособности от информационной инфраструктуры обеспечила условия, при которых угрозы информационной безопасности становятся в настоящее время одним из основных факторов, подрывающих стабильность развития компаний.

Деятельность любого современного сотрудника образовательной организации прямо или косвенно связана со сбором, хранением и обработкой информации.

Данная тенденция обусловливает внимание государства и общества к формированию нормативной базы, совершенствованию системы защиты информации и организации подготовки кадров в области информационной безопасности. В соответствии с Доктриной информационной безопасности РФ (утв. Президентом РФ 09.09.2000 г. № Пр-1895) актуальной остается задача создания единой системы подготовки кадров в области информационной безопасности и информационных технологий, обеспечивающей не только подготовку квалифицированных специалистов в области информационной безопасности и защиты информации, но и

изучение проблематики информационной безопасности всеми категориями специалистов, подготавливаемых в системе профессионального образования.

Таким образом, наряду с общей информационной подготовкой сотрудников образовательной организации, актуальной становится необходимость ее логического продолжения – формирования профессиональной компетентности в области информационной безопасности.

**Степень разработанности проблемы.** Отечественные и зарубежные исследования, связанные с проблематикой информационной безопасности (далее ИБ), широко раскрывают следующие вопросы:

– общие научные и методологические вопросы ИБ поднимаются в трудах А.П. Коваленко[43], Е.Б. Белов[13]; Р. В. Мещерякова[62], А.А. Шелупанова; В.П. Шерстюк[88], W. Stallings [4] и др.);

– аспекты нормативно-правового обеспечения ИБ (С.Л. Зефиров[38], В. М. Алексеев; Ю. М. Батурин[12]; Т.А. Кондратьева, В. С. Горбатов[28]; О. А. Городов[29], Р. И. Дремлюга[33], Ю. А. Журавлев[34], Г. О. Крылов[51], Т. А. Полякова[67], D. B. Thaw[5] и др.);

– аспекты ИБ как педагогической проблемы (Р. В. Амелин[6], А. А. Журин[35], П. Н. Корнюшин[46], А. А. Марков[60], В. А. Семененко[71], В. Н. Ясенев[91] и др.);

– проблемы подготовки кадров и формирования компетентности в области ИБ (А.П. Коваленко[47], Е. Б. Белов[45]; Е. Н. Бояров[19], А.С. Доронин[32], Э. В. Танова[74], E. Albrechtsen [1] и др.);

– практические аспекты ИБ и защиты информации (В. А. Галатенко[24], В.Н. Максименко, А. П. Даньков[30], Б.И. Скородумов А. А. Круглов[50], А. В. Крысин[52], В. П. Мельников[61], Ю. С. Уфимцев[76], В. Л. Цирлов[87] и др.);

Однако в научной литературе также отмечается, что в настоящее время вопросам целенаправленного формирования компетентности в области

информационной безопасности в педагогических исследованиях уделяется недостаточно внимания.

**Объект исследования –** система профессиональной подготовки сотрудников в ВУЗе.

**Предмет исследования** – процесс формирования компетентности в области информационной безопасности среди сотрудников в условиях вузовского образования.

**Цель исследования –** на основе теоретического анализа литературы разработать и внедрить технологию формирования компетенций в области информационной безопасности среди сотрудников образовательной организации.

**Гипотеза исследования** - если технология формирования компетентности в области информационной безопасности включает в себя совокупность специфических форм, методов и средств, то это будет способствовать

Для реализации цели были поставлены следующие **задачи**, которые и определили структуру работы:

1) Дать определение терминов компетентность, компетенция, раскрыть сущность, основные принципы компетентностного подхода.

2) Раскрыть составляющие профессиональной компетенции сотрудников образовательной организации в области информационной безопасности.

3) Разработать программу формирования компетентности сотрудников в области информационной безопасности.

4) Разобрать структуру образовательной организации и на основе этого сформулировать цели и задачи педагогического эксперимента.

5)В рамках педагогического эксперимента провести опытно-экспериментальную работу по внедрению технологий формирования компетенций, описанных ранее.

**Методологической основой исследования явились:**

– концепции развития научного знания (Т. Кун[54], И. Лакатос[57], М. Полани[65], К. Поппер[68], П. Фейрабенд[85] и др.), позволяющие рассматривать педагогическое знание в становлении и развитии;

– деятельностный подход к определению целей и задач профессиональной подготовки специалиста (А. Г. Асмолов[9], А. А. Вербицкий[21], Л. С. Выготский[23], П. Я. Гальперин[26], А. Н. Леонтьев[58], Н. Ф. Талызина[73] и др.), позволяющий определить структуру содержания подготовки, а также выделить этапы познавательной деятельности;

– личностно-ориентированный подход к профессиональной подготовке специалиста (Е. В. Бондаревская[17], А. В. Петровский[64], И. С. Якиманская[90] и др.), позволяющий организовать обучение с учетом индивидуальных особенностей обучающихся;

– системный подход к изучению процессов и явлений (В. Г. Афанасьев[10], Э. Г. Юдин, И. В. Блауберг[15] и др.), позволяющий рассматривать профессиональную подготовку специалиста как целостную систему.

**Теоретическую основу исследования** составили:

– теоретические положения компетентностного подхода (В. И. Байденко[11], Э. Ф. Зеер[37], И. А. Зимняя[39], Д. А. Иванов[40], А. В. Хуторской[86], В. В. Щербакова[89], Дж. Равен[70] и др.) и контекстного (Г. М. Андреева[7], М. Д. ИльязоваА. А. Вербицкий[22], А.А Бодалев[16], Н.Б. Лаврентьева, Г. В. Лаврентьев[55], Л. В. Львов[59] и др.) подходов к профессиональной подготовке специалистов;

– исследования в области организации обучения и применения педагогических технологий в системе высшего профессионального образования (В. П. Беспалько[14], М. В. Буланова-Топоркова[20], В. В. Краевский[49], Г. В. Лаврентьев, Н. Б. Лаврентьева[56], В. А. Сластенин[72], П. А. Юцявичене и др.);

– исследования методологии моделирования в педагогике (С. И. Архангельский[8], О. А. Козырева, Н. В. Кузьмина[53] и др.);

– фундаментальные исследования в области информационной безопасности (А. И. Коробеев[48], Я. О Кучина Р. И. Дремлюга, А. С. Забабурин, О. В. Казарин[42], T. R. Peltier [2], D. Salomon[3] и др.);

– работы в области обучения основам информационной безопасности (В.П. Лось, Е. Б. Белов[44], В. А. Галатенко[25], П. Н. Корнюшин[47], В. А. Семененко и др.);

**Экспериментальная база исследования:**

Филиал ВУНЦ ВВС «ВВА» в г.Челябинске

# ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ПРОБЛЕМЫ ФОРМИРОВАНИЯ КОМПЕТЕНТНОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1.1 Понятия компетенции и компетентности

Использование в современной педагогической литературе указанных в названии материала терминов тесно связано с процессом переориентации российского образования со «знаниевого» на компетентностный подход, что является необходимым условием модернизации и приведения его результатов в соответствие с международными стандартами.

Часто синонимически используемые понятия «компетенция» (не следует путать с правовым значением слова: «компетенция органов местного самоуправления» и пр.) и «компетентность» необходимо различать:

Компетенция включает совокупность взаимосвязанных качеств личности (знаний, умений, навыков, способов деятельности), задаваемых по отношению к определенному кругу предметов и процессов и необходимых для качественной продуктивной деятельности по отношению к ним.

Компетентность – владение, обладание человеком соответствующей компетенцией, включающей его личностное отношение к ней и предмету деятельности.

Об этом подробно рассказывается, например, на страницах учебного пособия для вузов «Основы педагогического мастерства» Л.В. Заниной и Н.П. Меньшикова[38], а также в статьях Д.А. Иванова[41] и других книгах и статьях, перечисленных в данном библиографическом материале.

Если обратиться к словарям, то наиболее часто употребляемое словосочетание со словом «компетентность» профессиональная компетентность учителя трактуется как «владение учителем необходимой суммой знаний, умений и навыков, определяющих сформированность его педагогической деятельности, педагогического общения и личности учителя как носителя определенных ценностей, идеалов и педагогического сознания».

Подобное определение дает и кандидат педагогических наук, старший научный сотрудник лаборатории дидактики Института Теории образования и Педагогики РАО, Генике Е.А.[27] в своей книге «Профессиональная компетентность педагога», указывая на то, что соотношение этих составляющих должно быть равномерным. Это и будет интегративной компетентностью педагога.

Что касается наиболее употребительного словосочетания «ключевые компетенции», то в европейском проекте «Определение и отбор ключевых компетенций» они определяются как важные «во многих жизненных сферах и служащие залогом жизненного успеха и эффективного функционирования общества».

Для оценки эффективности деятельности граждан, работников организаций в информационном обществе предлагается использовать новую, адекватную современным условиям интегративную характеристику личности – компетентность.

Данная характеристика эффективности деятельности послужила основанием для разработки новых критериев отбора людей на ведущие позиции в обществе, для поощрения роста качества поведения и деятельности граждан, работников конкретных организаций.

Компетентность как интегральная характеристика эффективности деятельности (поведения) человека, мера успешности достижения цели является предметом и объектом изучения многих наук.

Освоение знаний, умений, навыков, способов разрешения проблем, правил жизни в обществе, приобретение определенных личностных качеств – условие жизнедеятельности. Как правило, любая человеческая деятельность оценивается обществом. Основной мерой выступает компетентность. Завершение определенного уровня образования и достижение соответствующих личностных качеств фиксируется обществом через присвоение человеку должной квалификации, ученого или военного звания,

ученой степени и т. п.: личность наделяется полномочиями на основе уровня освоенных компетенций.

Данное понимание компетенций требует уточнения, которое может быть осуществлено включением в когнитивные и аффективные составляющие сформированности у личности ценностных отношений к знаниям, умениям и навыкам. В таком случае компетенции могут характеризовать не только формально круг полномочий, которыми наделяется личность, но и морально-ценностный аспект (диплом врача дает право занимать определенную должность в лечебном учреждении, но уровень его отношений к собственным решениям, имеющимся знаниям формирует иной облик – врача с морально ценностным правом быть им).

В отечественной педагогической практике исследованию компетенций в образовании посвящается увеличивающее количество научных работ, что обусловило выделение компетентностного подхода в качестве самостоятельного.

На основе анализа источниковой базы исследования определены этапы возникновения, становления и развития компетентностного подхода в отечественной системе образования:

I этап (1960 — 1970 гг.) характеризуется введением в научный оборот терминов «компетенция», «компетентность» (коммуникативная), поиском дифференциации сущности понятий «компетентность» и «компетенция». В ходе этого этапа исследователи стремились выявить и обосновать теоретико-методологические подходы к практическому использованию указанных понятий в интересах профессиональной подготовки различных категорий специалистов. В частности, были выделены отраслевой, функциональный и компетентностный подходы.

Стремительные прорывы страны в космическое пространство (1961), мощная армия и флот, утверждение Морального кодекса строителя коммунизма (1961) и многочисленные достижения в иных сферах жизнедеятельности государства, общества и личности способствовали

утверждению в системе профессионального образования страны отраслевого подхода. В соответствии с государственным заказом и квалификационными требованиями к выпускникам образовательные учреждения начального, среднего и высшего профессионального образования производили отраслевых специалистов универсального типа.

II этап (1970 - 1990 гг.) характеризуется распространением понятий «компетенция» и «компетентность» на теорию, практику и методику обучения и воспитания, на сферу профессионального управления. На партийных съездах этого этапа развития страны в теории, а в трудовых коллективах на практике выделялись наиболее компетентные руководители. Искомые понятия дополнялись производными от них: «социальными компетенциями», «социальными компетентностями»1.

Изменившиеся социально-экономические и образовательные условия в стране способствовали выделению в 1980-е гг. функционального подхода, который фокусировал подготовку конкретных специалистов какой-либо отрасли на их функциях или функциональном предназначении. Несмотря на значительные отраслевые и личные трудовые свершения, «функциональные» специалисты часто не имели представлений, знаний, умений и навыков, которыми обладали их коллеги из смежных отраслей, ведомств и т.д.

В результате порой приходилось вновь «изобретать велосипед» и при этом нести личную ответственность не только за свои трудовые свершения, но и за успехи руководимых коллективов. Кстати основу содержания ГОС ВПО первого и второго поколений составлял именно функциональный подход к подготовке различных категорий специалистов.

III этап (с 1990-х гг.) характеризуется становлением профессиональной компетентности. Были сформированы принципы: научиться познавать; делать - «от понятия квалификации к понятию компетентности»...; жить вместе (с другими)... и учиться жить. Причем, делать так, чтобы приобрести не только профессиональную квалификацию, но и компетентность, дающую возможность справляться с различными ситуациями и работать в группе 2.

Однако усилия Международной комиссии по образованию не привели к выработке единых взглядов на сущность компетентностного подхода и составляющих его понятий «компетенция» и «компетентность» в различных областях образовательной и профессиональной деятельности.

В соответствии с решением коллегии Минобразования РФ от 1 февраля 2000 г. № 2/2 «Об утверждении государственных образовательных стандартов высшего профессионального образования» был установлен перечень специальностей ВПО по направлению «Информационная безопасность», который составили: «Криптография», «Компьютерная безопасность», «Организация и технология защиты информации», «Комплексная защита объектов информации», «Комплексное обеспечение информационной безопасности автоматизированных систем» и «Информационная безопасность телекоммуникационных систем».

В процессе анализа данных, представленных на сайтах профильных российских вузов, занимающихся подготовкой специалистов по направлению «Информационная безопасность», были выявлены условия, способствующие обеспечению качественной подготовки СПИБ:

-во-первых, связанные с обеспечением взаимосвязи реализуемого вузами образовательного процесса с результатами научных исследований в области информационной безопасности. Генерирующими являются сложившиеся научные школы: в области криптографии при ИКСИ ФСБ России1; в области технических средств защиты при Московском инженерно-физическом институте; в области государственно-правового регулирования защиты информации при МГУ им. М.В. Ломоносова и защиты компьютерных систем от вредоносных программ при Санкт-Петербургском государственном политехническом университете;

- во-вторых, всестороннее материально-техническое обеспечение образовательного процесса, включая ознакомление будущих специалистов с отечественными разработками типа «Гриф», «Кондор»3, комплексной системой защиты информации «Панцирь» (операционной системы Windows

2000 /XP/ 2003, электронным замком «Соболь» (аппаратно-программное средство защиты компьютера от несанкционированного доступа) и др.;

- в-третьих, обеспечение образовательного процесса профильных вузов высококвалифицированным профессорско-преподавательским составом (педагогическими работниками) в соответствии с требованиями ФГОС ВПО.

Вместе с тем для подготовки современных СПИБ требуются не только высококвалифицированные педагогические работники и выдающиеся ученые, но и практики, способные созидать на высоком профессиональном уровне.

Следовательно, сущность компетентностного подхода в подготовке СПИБ должна отражать, прежде всего, национальные условия его реализации и реальную практику. Этот вывод следует из особенностей информационной безопасности1, как вида национальной безопасности. Профессиональная компетентность СПИБ может определяться через анализ характеристик его профессиональной деятельности (ПЗУН, личный опыт, способности, поведение, этика, ментальность, ответственность) различными методами при решении конкретных задач.

## 1.2. Компетентность сотрудников образовательной организации в области информационной безопасности

В педагогических вузах актуализируются новые требования к профессиональной подготовке выпускников. Для специалистов в области педагогического образования основным полем деятельности является педагогика, психология, методика обучения и воспитания, а информационная безопасность личности учащихся лишь один из способов достижения педагогических целей.

Обеспечение информационной безопасности личности педагога может быть достигнуто путем введения в соответствующие стандарты образования соответствующих компетенций, направленных на формирование информационной культуры специалиста с обязательной составляющей компетентностью в области информационной безопасности личности.

Таким образом, Федеральные образовательные стандарты разных ступеней образования и образовательные программы, разработанные на из основе, в обязательном порядке должны содержать требования, касающиеся компетенций в области информационной безопасности, причем данные компетенции следует отнести к категории общекультурных.

Следует отметить, что в существующих ФГОС проблемам ИБ уделено недостаточное внимание, которое ограничивается формированием способности «понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12)». Однако определенное нами ранее содержание профессиональной компетентности сотрудников в области ИБ позволяет сделать вывод, что этого недостаточно. Данную мысль подтверждает В. П. Поляков[66], который отмечает, что в настоящее время подготовка специалистов соответствующего профиля в области ИБ не имеет системного характера.

Профессиональная компетентность в области ИБ - это многофакторное явление, включающее в себя систему теоретических знаний в области ИБ и способов их применения в конкретных рабочих ситуациях, а также ценностные ориентации, связанные с аспектами ИБ в профессиональной деятельности. Таким образом, анализ источников по вопросам профессиональной компетентности, профессиональной подготовки специалистов, анализ содержания ИБ в профессиональной деятельности сотрудников, позволяют нам выделить следующие сущностные характеристики:

1. Мотивационные характеристики отражают направленность будущих специалистов на осуществление деятельности но защите профессионально значимой информации, потребности, мотивы, стремления, интерес к образованию и самообразованию в области ИБ, а также морально-этические установки в этом аспекте.

2. Когнитивные характеристики отражают знания о сущности проблемы обеспечения ИБ; знания об основных угрозах для информационных ресурсов в сфере экономики; основы правового обеспечения ИБ, в том числе российского и зарубежного законодательства, конституционные нормы, законы РФ и указы президента РФ, требования руководящих документов совета безопасности РФ и других органов государственного управления, ответственность за компьютерные преступления; принципы и содержание организационного обеспечения ИБ (политика безопасности, контроль, разграничение и ограничение доступа к информационным ресурсам и т.п.).

3. Деятельностные характеристики включают комплекс умений и навыков осуществления мероприятий по обеспечению ИБ в профессиональной деятельности: нормативно-правовых (определение полномочий, разграничение доступа, определение порядка контроля, документирования и анализа действий и пр.), административных (мероприятия, осуществляемые при проектировании и разработке правил и

инструкций по ИБ, организация охраны, учета, хранения, использования и уничтожения документов и носителей информации и пр.), физических (применение механических, электро-, электронно-механических устройств, создающих физические препятствия для доступа к защищаемой информации и компонентам системы, а также средств визуального наблюдения, связи и сигнализации), программно-аппаратных (использование электронных устройств и программ, которые реализуют идентификацию, аутентификацию, авторизацию субъектов ИБ, разграничение доступа, регистрацию и анализ событий, криптографическую обработку и пр.).

Формирование профессиональной компетентности в области ИБ среди сотрудников образовательных организаций выявляет необходимость определения критериев, показателей и уровней сформированное данной компетентности.

Вопросам определения критериев и показателей сформированности компонентов профессиональной деятельности посвящен целый ряд публикаций отечественных исследователей, таких как В. А. Беликов, в. П. Беспалько, П.Я. Гальперин, В. А. Сластенин, Н. Ф. Талызина и др. Э. Ф. Зеер отмечает, что критерий «выступает как основа для любой классификации и представляет собой однородную в основе качественную характеристику явления или понятия. Он выступает как обобщенный показатель одних и тех же или аналогичных систем, позволяющий их дифференцировать», а показатель - это «свойство, признак изучаемого объекта, количественная или качественная характеристика которого описывает феномен в терминах критериальной оценки».

В педагогических вузах актуализируются новые требования к профессиональной подготовке выпускников. Для специалистов в области педагогического образования основным полем деятельности является педагогика, психология, методика обучения и воспитания, а информационная безопасность личности учащихся  лишь один из способов достижения педагогических целей.

Тем временем, в современном мире возрастает количество преступлений в области информационной безопасности. Основываясь на нормативно-правовых актах и статистике использования учащимися ресурсов информационно-телекоммуникационных сетей, можно сделать вывод, что обеспечение информационной безопасности образовательной организации – это целый комплекс мер, направленных как на предотвращение мошенничества в информационной сфере, неправомерный доступ к конфиденциальной информации, так и на минимизирование нежелательного информационного воздействия на учащихся. Подобные вызовы современного медиа-пространства, применимо к образовательной организации решаются комплексом организационных и технических средств, а также формированием среди учащихся и преподавателей компетенций в области информационной безопасности в условиях развивающегося медиа-пространства.

Если оценить значимость принимаемых мер по обеспечению информационной безопасности в образовательной организации, то становится очевидно, что формирование компетенций у учащихся более значимо, чем применение технических средств и соблюдение организационных мер, ведь угрозы не заканчиваются на антивирусной защите и организационных мерах.

Таким образом педагог должен давать учащимся знания и формировать навыки безопасного использования информации в окружающем медиа-пространстве, которые позволили бы учащемуся самостоятельно оценивать риски того или иного ресурса в глобальной сети, противостоять злоумышленникам, а также самостоятельно организовывать учебную деятельность с использованием ресурсов…

Для этого преподаватель должен дать учащемуся знания об основных аспектах информационного взаимодействия в современном мире, а также об актуальных угрозах, возникающих в процессе обучения.

В современном мире существует множество способов информационного мошенничества, посредством сетевых атак, рассмотрим наиболее часто встречающиеся из них[18]. На данный момент выделяют следующие атаки: mailbombing, переполнение буфера, использование специализированных программ (вирусов, снифферов, троянских коней, почтовых червей, rootkit-ов и т.д.), сетевая разведка, IP-спуфинг, man-in-the-middle, инъекция (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция), отказ в обслуживании (DoS- и DDoS-атаки), phishing-атаки.

Атака mailbombing строится на высылании на почтовый ящик «жертвы» огромного количества писем, в результате чего может быть выведен из штатного режима функционирования, как конкретный ящик, так и весь почтовый сервер. Для реализации данной атаки не требуется высокий навык у нарушителя, а достаточно иметь доступ к серверу, позволяющему отправлять постовые сообщения анонимно. Защита от данной атаки со стороны пользователя довольно проста: указывать электронный адрес своего почтового ящика только в проверенных источниках.

Атака с переполнением буфера строится на уязвимости разного программного обеспечения, которое позволяет достичь предел раздела буферной памяти и аварийно завершить работу приложения или позволить нарушителю выполнить команду с правами пользователя, под которым в данный момент работал пользователь. Для реализации данной угрозы необходим высокий навык нарушителя, знание уязвимостей в коде программ, установленных на ПК «жертвы». Пользователю, вследствие низкого уровня знаний в области программного кода, трудно эффективно противостоять данной атаке, но с помощью использования официальных версий программ и своевременного обновления их, можно свести риск к минимуму.

Самым распространённым видом сетевых атак являются атаки с использованием вредоносного программного обеспечения. По своему воздействию компьютерные вирусы разделяются на несколько видов, но

объединяет их то, что данные программы действуют на ПК «жертвы» без согласия пользователя и своей целью несут уничтожение информации, снижение производительности ЭВМ, передачу конфиденциальной информации без ведома пользователя и прочие негативные воздействия на программное обеспечение. Подобные программы могут модифицировать файлы операционной системы, являться частью программ, которые пользователь использует осознанно и при этом отправлять данные адресатам по сети, без уведомления пользователя, а также маскировать своё присутствие на ПК пользователя, посредством модификации реестра операционной системы, стека сетевых протоколов и прочего. Защита от данных уязвимостей для пользователя заключается в отказе от скачивания каких либо программ из непроверенных источников, использовании антивирусных программ на ПК, а также поверхностного анализа работы операционной системы. В случае резкого уменьшения быстродействия системы, в особенности после установки программ от непроверенного издателя, следует как можно скорее проверить антивирусной программой память устройства, с целью найти и обезвредить вредоносные программные средства.

Атака man-in-the-middle действует согласно своему названию – человек посередине. Злоумышленник, используя незащищённый канал связи, внедряется в него между «жертвой» и ресурсом, который она запрашивает. Все пакеты трафика проходят через устройства преступника и если они не защищены, он без труда считывает содержащуюся в них информацию. Нетрудно догадаться, что данная атака позволяет злоумышленнику получить полный доступ к информации пользователя, паролям к защищаемым ресурсам и прочим конфиденциальным данным. Защита от данной угрозы состоит в шифровании сетевого трафика, будь то использование приложений с шифрованием, так и обмен сообщениями заранее зашифрованными перед отправкой.

Одной из самых известных сетевых атак является DoS-атака. Она нацелена на то, чтобы сделать сетевой ресурс недоступным, вследствие перегрузки его огромным количеством входящих запросов. Данная атака опасна простотой реализации и низкой требовательностью к навыкам злоумышленника. Защититься от этой атаки со стороны пользователя достаточно сложно, так как весь трафик, который провайдер пропустит к пользователю – дойдёт до адресата и ресурсы пользователя будут перегружены запросами. Посильной защитой от подобного со стороны пользователя является не указывать названия своих ресурсов в непроверенных источниках, а также резервное копирование критически важной информации.

Phishing – атаки направлены на обман пользователей, путём использования ссылок либо похожих на общеизвестные, либо ведущих на другой сайт. Простым примером будет создание домена, минимально отличающегося от общеизвестного, а затем письмо пользователям этого домена с просьбой перейти по ссылке и изменить свои парольные данные. В таком случае, злоумышленник легко получит доступ к информации, вводимой пользователем. Защитой от подобной атаки будет тщательная проверка адресов в подобных ссылках, а также перепроверка данной информации в других, проверенных информационных источниках (служба поддержки, официальный телефон банка, прочее).

Все мы живём в правовом государстве, поэтому обучаемый должен давать правовую оценку как своим действиям, так и действиям злоумышленников, касаемо информационной безопасности. Это важно как для недопущения нарушений действующего законодательства в данной сфере, так и знания об ответственности злоумышленников за их деяния, с целью не допустить мошенничества полученной незаконным путём информацией.

Основными правовыми актами, регулирующими вопросы информационной безопасности в Российской Федерации являются:

- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»[82]
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г.)[83]
- Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ[81]
- Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (с изменениями от 2 февраля, 18 декабря 2006 г., 24 июля 2007 г.)[84]
- Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)[31]
- УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ[75]

Остановимся более подробно на каждом из этих законодательных актов. Таким образом, Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – 149-ФЗ) дает нам основные определения понятий, связанных с правовым регулированием информации. Также 149-ФЗ обозначает основные принципы правового регулирования информации, такие как свобода её поиска, установление ограничения доступа к информации, на основе только федеральных законов, достоверность и своевременность предоставления информации, и одно из самых важных – неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица, без его на то согласия.

149-ФЗ – закон, дающий правовую оценку многим аспектам информационного взаимодействия и в его тексте обучаемые могут найти ответы на вопросы, как об обладании информации, её предоставлении и

распространении, так и о государственном регулировании в сфере применения информационных технологий.

Федеральный закон № 152-ФЗ «О персональных данных» (далее – 152-ФЗ) даёт правовую оценку персональных данных, а именно, любой информации, которая прямо или косвенно относится к определяемому физическому лицу – субъекту персональных данных. Данный правовой акт очень важен для каждого гражданина, так как его данные – охраняемая законом информация и он вправе требовать соблюдения установленных правил её обработки, в то же время зная основные положения, обучаемый сможет не допустить изменения статуса личной информации с охраняемой законом на общедоступную. 152-ФЗ регулирует принципы и условия обработки персональных данных, объясняет права субъекта персональных данных, а также обязанности оператора информационной системы персональных данных.

Вспоминая основные сетевые угрозы и опираясь на определения из 152-ФЗ, можно сказать, что персональные данные – очень важная часть информационно безопасности каждого физического лица. Утеря конфиденциальности этой информации может вести как к реализации угроз интернет мошенничества, утере тайны частной жизни, так и к прямым потерям финансовых средств, таким как операции с банковскими счетами, используя биометрические персональные данные.

Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ регулирует вопросы электронной подписи, а именно - информации, которая используется для определения лица, подписывающего информацию. Технология цифровой подписи всё сильнее внедряется в нашу жизнь, как на рабочих местах, за счёт информатизации и автоматизации процесса документооборота, так и в повседневной жизни для доступа к порталам государственных услуг.

Часто, после окончания образовательных учреждениях работают на предприятиях и сталкиваются с понятием «коммерческая тайна». Вопросы,

связанные с ним регулирует федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (далее – 98-ФЗ). Этот нормативный акт даёт определения конфиденциальной информации, которая является собственностью обладателя, позволяющая получить коммерческую выгоду. Будущий работник, опираясь на положения 98-ФЗ сможет определять, какая информация является коммерческой тайной, как следует выполнять требования по сохранению её конфиденциальности, а также в случае неправомерного присвоения к информации ограничительной пометки «Коммерческая тайна», оспорить действия работодателя.

За нарушение каждого из вышеперечисленных законов предусмотрена дисциплинарная, административная, а также уголовная ответственность. Рассмотрим главу 28 Уголовного Кодекса Российской Федерации, посвященную преступлениям в сфере компьютерной информации.

Глава содержит 4 статьи, первая из них, 272 направлена на преступления связанные с неправомочным доступом к компьютерной информации. Таким образом, уничтожение, блокирование, модификация или копирование защищённой законом информации может быть наказано сроком лишения свободы, вплоть до 7 лет, если преступное деяние проходило с использованием служебного положения, группой лиц, из корыстной заинтересованности и ущерб от этих действий составил более миллиона рублей. Примечательно то, что наказаны могут быть даже действия, направленные на копирование информации, защищённой законом, будь то персональные данные, либо коммерческая тайна предприятия.

Статья 273 УК РФ описывает ответственность за преступления связанные с созданием, использованием и распространением вредоносных компьютерных программ. Наказание за эти деяния могут составлять до 7 лет лишения свободы, в случаях, если преступление повлекли тяжкие последствия, либо создали угрозу их наступления.

Статья 274 УК РФ описывает наказание за преступления. Связанные с нарушением правил эксплуатации средств хранения, обработки или передачи

компьютерной информации и информационно-телекоммуникационных сетей. Нарушение данных законов влечёт за собой наказание в виде лишения свободы на срок до 5 лет.

Как правило, большая часть обучаемых понимает назначение и принцип действия программных средств защиты информации (антивирус, антиспам, прочее), в то время, как проблеме информационного воздействия на личность человека уделяется гораздо меньшее внимание. Важной частью обеспечения информационной безопасности личности обучаемого является осознание возможности угроз, связанных с манипуляциями его сознанием. Подобные угрозы могут исходить как от конкретных людей, так и в целом, от медиа-пространства, СМИ и в худшем случае от запрещенных организаций. В процессе обучения студент учится мыслить критически, проверять информацию о предметах и явлениях, поэтому

Обеспечение информационной безопасности личности педагога может быть достигнуто путем введения в соответствующие стандарты образования соответствующих компетенций, направленных на формирование информационной культуры специалиста с обязательной составляющей компетентностью в области информационной безопасности личности.

Таким образом, Федеральные образовательные стандарты разных ступеней образования и образовательные программы, разработанные на из основе, в обязательном порядке должны содержать требования, касающиеся компетенций в области информационной безопасности, причем данные компетенции следует отнести к категории общекультурных.

### 1.3. Программа формирования компетентности сотрудников в области информационной безопасности в образовательной организации

Если обратиться к федеральному закону от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации"[77], в статье 27 раскрывается структура образовательной организации. Пункты 1 и 2 гласят: «

1. Образовательные организации самостоятельны в формировании своей структуры, если иное не установлено федеральными законами.

2. Образовательная организация может иметь в своей структуре различные структурные подразделения, обеспечивающие осуществление образовательной деятельности с учетом уровня, вида и направленности реализуемых образовательных программ, формы обучения и режима пребывания обучающихся (филиалы, представительства, отделения, факультеты, институты, центры, кафедры, подготовительные отделения и курсы, научно-исследовательские, методические и учебно-методические подразделения, лаборатории, конструкторские бюро, учебные и учебно-производственные мастерские, клиники, учебно-опытные хозяйства, учебные полигоны, учебные базы практики, учебно-демонстрационные центры, учебные театры, выставочные залы, учебные цирковые манежи, учебные танцевальные и оперные студии, учебные концертные залы, художественно-творческие мастерские, библиотеки, музеи, спортивные клубы, студенческие спортивные клубы, школьные спортивные клубы, общежития, интернаты, психологические и социально-педагогические службы, обеспечивающие социальную адаптацию и реабилитацию нуждающихся в ней обучающихся, и иные предусмотренные локальными нормативными актами образовательной организации структурные подразделения).»

Опираясь на эти выписки из федерального закона, мы можем понять, что структура образовательной организации определяется в первую очередь уставом образовательной организации, утвержденным её руководителем. В то же время, очевидно, что для полноценного функционирования образовательной организации высшего образования необходимо создание структурных подразделений, как обеспечивающих проведение образовательного процесса, так и непосредственно включающих в себя профессорско-преподавательский состав.

Вопрос разделения сотрудников образовательной организации высшего образования по структурным подразделениям раскрывается в

квалификационных характеристиках должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования, утвержденных Приказом Минздравсоцразвития России от 11.01.2011 № 1н[69]. Данные квалификационные характеристики применяются для 3 категорий сотрудников, которые приведены в таблице 1.


Таблица 1

Наиболее подробно квалификационные требования к профессорско-преподавательскому составу изложены в Федеральном государственном образовательном стандарте высшего образования по направлению подготовки 44.03.01 Педагогическое образование (уровень бакалавриата)[78] (Далее – ФГОС ВО 44.03.01). Данный ФГОС ВО 44.03.01 введён приказом Министерства образования и науки от 4 декабря 2015г №1426, взамен утратившего силу федерального государственного образовательного стандарта высшего образования по направлению подготовки 050100 Педагогическое образование (квалификация (степень) бакалавр)[79], и представляет собой совокупность требований, обязательных для реализации образовательной программы по подготовке будущих педагогов, которые и

составят профессорско – преподавательский состав образовательной организации, после получения высшего образования.

Рассмотрим подробнее федеральные государственные образовательные стандарты высшего образования, чтобы понять, какими компетенциями должны обладать сотрудники из числа профессорско-преподавательского состава. Таким образом в федеральном государственного образовательном стандарте высшего образования по направлению подготовки 050100 Педагогическое образование (квалификация (степень) бакалавр) (Далее – ФГОС ВО 050100) указывается, что выпускник должен обладать 16 общекультурными компетенциями (ОК) , в числе которых есть «понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12)». В то время, как в ФГОС ВО 44.03.01 содержится уже 9 общекультурных компетенций, из которых только «способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве(ОК-3)» и «способность использовать базовые правовые знания в различных сферах деятельности (ОК-7)», наиболее подходят к целям формирования компетентности в области информационной безопасности.

Анализируя актуальные руководящие документы по подготовке профессорско-преподавательского состава, усматривается то, что проблемам формирования компетенций в области информационной безопасности уделено очень мало времени. Таким образом во ФГОС ВО 44.03.01 общекультурных компетенций у будущего педагога гораздо меньше в сравнении с ФГОС ВО 050100 (выведен из действия) и среди них не упоминается защита информации и умение противостоять актуальным информационным угрозам.

Для понимания знаний, обязанностей и требований профессорско-преподавательского состава обратимся к приказу Минздравсоцразвития РФ от 11.01.2011 N 1н "Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования".

В первую очередь рассмотрим должность преподавателя, которая составляет основу профессорско-преподавательского состава. Основываясь на вышеупомянутом документе преподаватель:

«Организует и проводит учебную и учебно-методическую работу по всем видам учебных занятий, за исключением чтения лекций. Участвует в научно-исследовательской работе кафедры, иного подразделения образовательного учреждения. Обеспечивает выполнение учебных планов и программ. Под руководством профессора, доцента или старшего преподавателя разрабатывает или принимает участие в разработке методических пособий по видам проводимых занятий и учебной работы, организует и планирует методическое и техническое обеспечение учебных занятий. Создает условия для формирования у обучающихся (студентов, слушателей) основных составляющих компетентности, обеспечивающей успешность будущей профессиональной деятельности выпускников. Принимает участие в воспитательной работе с обучающимися (студентами, слушателями), в организации их научно-исследовательской работы, в профессиональной ориентации школьников, в разработке и осуществлении мероприятий по укреплению, развитию, обеспечению и совершенствованию материально-технической базы учебного процесса, обеспечению учебных подразделений и лабораторий оборудованием. Контролирует и проверяет выполнение обучающимися (студентами, слушателями) домашних заданий. Контролирует соблюдение обучающимися (студентами, слушателями) правил по охране труда и пожарной безопасности при проведении учебных

занятий, выполнении лабораторных работ и практических занятий. Участвует в организуемых в рамках тематики направлений исследований кафедры семинарах, совещаниях и конференциях, иных мероприятиях образовательного учреждения.»

В должностных обязанностях преподавателя, как и старшего преподавателя, доцента, профессора основными являются обязанности по обеспечению учебного процесса, безопасному использования учебно-материальной базы при проведении занятий, участие в научно-исследовательской работе подразделения. Вопросам информационной безопасности в учебном процессе не было уделено должного внимания.

В свою очередь, более информативен раздел «должен знать», в каждом из перечисленных должностей профессорско-преподавательского состава. Рассмотрим это на примере квалификационных требований к должности профессор, так как к ней предъявляются наибольшие требования.

«Должен знать: законы и иные нормативные правовые акты Российской Федерации по вопросам высшего профессионального образования; локальные нормативные акты образовательного учреждения; теорию и методы управления образовательными системами; государственные образовательные стандарты высшего профессионального образования; порядок составления учебных планов; правила ведения документации по учебной работе; основы педагогики, физиологии, психологии; методику профессионального обучения; методы и способы использования образовательных технологий, в том числе дистанционных; основные методы поиска, сбора, хранения, обработки, предоставления, распространения информации, необходимой для осуществления научно-исследовательской деятельности; механизмы оформления прав интеллектуальной собственности; технологию организации методической, научно-методической, научно-исследовательской работы; современные формы и методы обучения и воспитания; правила и порядок представления обучающихся (студентов) к государственным и именным стипендиям;

нормативные документы, регламентирующие статус научных, педагогических и руководящих работников образовательных учреждений высшего профессионального образования, особенности регулирования их труда; основы управления персоналом; основы экологии, экономики, права, социологии; финансово-хозяйственную деятельность образовательного учреждения; основы административного, трудового законодательства; требования к работе на персональных компьютерах, иных электронно-цифровых устройствах; правила по охране труда и пожарной безопасности.»

Анализируя данную выписку, мы можем понять, что в требованиях к наиболее подготовленному члену профессорско-преподавательского состава к вопросам обеспечения информационной безопасности относятся только знания локальных нормативно правовых актов, знание методов сбора, обработки и использования информации, умение работать с персональными электронными вычислительными машинами. Этих знаний и навыков недостаточно для формирования у обучаемых твердых компетенций в области информационной безопасности.

Основываясь на требованиях ФГОС для будущих педагогов, а также на приказ Минздравсоцразвития РФ можно сделать вывод, что проблемам компетентности сотрудников образовательной организации уделено недостаточно много времени. Есть несколько путей решения данной проблемы: внесение изменений в образовательный процесс будущих педагогов (изменение дисциплин информационной направленности, добавление новых дисциплин), так и дополнительное образование при учреждениях высшего образования на непосредственном месте работы будущих педагогов.

Согласно ч. 2 п. 5 ст. 47 Федерального закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации", педагогический работник имеет право на дополнительное профессиональное образование по профилю педагогической деятельности не реже чем один раз в три года. В условиях работы в учебном заведении высшего образования, целесообразнее всего

было бы рассмотреть возможность проведения дополнительного профессионального образования на базе этого же учебного заведения.

Ранее были затронуты квалификационные требования к различным сотрудникам образовательной организации, таким как руководители, профессорско-преподавательский состав, работники административно-хозяйственного и учебно-вспомогательного персонала. Очевидно, что наибольшие требования к компетенциям в области информационной безопасности будут у профессорско-преподавательского состава, так как они непосредственно задействованы в учебном процессе и несут знания обучаемым.

В целях повышения компетенций в области информационной безопасности среди профессорско преподавательского состава, целесообразно провести курсы, которые включают в себя как лекционные, так и практические занятия. В рамках этих курсов будут рассмотрены нормативно-правовые акты в области информационной безопасности, основные угрозы информационной безопасности в образовательной организации, что должно повысить уровень соответствующих компетенций среди профессорско-преподавательского состава.

Приведу пример одной из лекций данного курса, которая затрагивает тему информационной безопасности в социальных медиа-ресурсах.

## ПЛАН – КОНСПЕКТ

### проведения занятия профессорско-преподавательским составом

**Тема: Организация информационной безопасности в социальных медиа-ресурсах сети «Интернет»**

**Занятие:** Лекция №2 курсов повышения квалификации

**Цели:**

1. Довести до профессорско-преподавательского состава информацию об угрозах информационной безопасности в социальных медиа-ресурсах сети Интернет.
2. Довести до профессорско-преподавательского состава информацию о перечне сведений, опубликование которых создает предпосылки к разглашению информации ограниченного доступа.
3. Довести до профессорско-преподавательского состава рекомендации по использованию социальных медиа-ресурсов сети Интернет сотрудниками образовательной организации.

**Учебные вопросы:**

1. Угрозы информационной безопасности в социальных медиа-ресурсах сети Интернет.
2. Перечень сведений, опубликование которых создает предпосылки к разглашению информации ограниченного доступа.
3. Рекомендации по использованию социальных медиа-ресурсов сети Интернет сотрудниками образовательной организации.

**Время проведения:** 20 мин

**Место проведения:** конференц-зал

**Материальное обеспечение:**

1. Мультимедийная аппаратура (слайдовая презентация).

## ХОД ЗАНЯТИЯ

**I. Вводная часть – 1 мин.**

1. Проверить наличие обучаемых.
2. Объявить тему и цель занятия, время и порядок проведения.
3. Вступление.

Основными задачами по обеспечению информационной безопасности в социальных медиа-ресурсах сети Интернет является предотвращение утечки информации ограниченного доступа, способной нанести ущерб безопасности образовательной организации.

**II. Основная часть – 18 мин.**

**1 учебный вопрос** (4 мин): **Угрозы информационной безопасности в социальных медиа-ресурсах сети Интернет**

Угрозами информационной безопасности в социальных медиа-ресурсах сети Интернет являются:

1. Несанкционированный доступ к персональным компьютерам и мобильным устройствам сотрудников образовательной организации, с которых осуществляется посещение социальных медиа-ресурсов сети Интернет.

2. Несанкционированный доступ к контенту, размещаемому сотрудниками образовательной организации в социальных медиа-ресурсах сети Интернет.

3. Определение актуального местоположения сотрудников образовательной организации с преступными целями.

4. Утечка информации ограниченного доступа через социальные медиаресурсы сети Интернет при размещении данной информации сотрудниками образовательной организации в социальных медиа-ресурсах сети Интернет.

5. Идентификация должностных лиц сотрудниками образовательной организации в социальных медиа-ресурсах сети Интернет.

6. Размещение информации, содержащей сведения, компрометирующие или дискредитирующие деятельность образовательной организации.

Информационная безопасность в социальных медиа-ресурсах обеспечивается мерами направленными на исключение:

- разглашения информации, ставшей им известной по работе, а также иной информации служебного характера;

- размещения информации, дискредитирующей имидж образовательного учреждения, руководства Минобрнауки России и других должностных лиц образовательной организации;

- размещения персональных данных о сотрудниках образовательной организации, а также фото-, аудио- и видеоматериалов с их участием и указанием персонифицирующей информации без их согласия.

**2 учебный вопрос** (4 мин): **Перечень сведений, опубликование которых создает предпосылки к разглашению информации ограниченного доступа и дискредитации имиджа образовательной организации**

К сведениям (персональным данным), позволяющим идентифицировать должностных лиц Вооруженных Сил относится:

- фамилия, имя, отчество;

- год, месяц, дата и место рождения;

- адрес проживания (регистрации);

- номер телефона (мобильный, рабочий, служебный, домашний, и т.п.); адрес электронной почты;

- семейное, социальное, имущественное положение;

- образование (где и когда получено образование, полученные специальности);

- трудовая деятельность (срок, место работы, наименование образовательных учреждений);

- профессия, должность, место работы ;

- сведения о доходах, банковских счетах и картах; сведения о состоянии здоровья;

- фото-, аудио- и видеоматериалы, сделанные на рабочем месте, в местах командировок, а также с указанием информации, содержащей географические координаты своего местонахождения, указанных объектов, мест.

К сведениям, опубликование которых создает предпосылки к дискредитации имиджа образовательной организации, политического руководства страны, руководства Минобрнауки России и других должностных лиц относится:

информация, компрометирующая политическое руководство государства, Министерство образования и науки, должностных лиц ;

- информация, содержащая сведения, характеризующие деятельность образовательной организации;

- информация, пропагандирующая насилие, порнографию, унижение человеческого достоинства, безнравственное поведение, нецензурную брань и др.;

- информация, содержащая оценку решений политического руководства государства, непосредственного руководства;

- информация, размещаемая должностными лицами в ходе участия в интернет-сообществах по принадлежности к учебным заведениям;

- информация третьих лиц (родственников, коллег, друзей, знакомых и других), содержащий сведения, персонифицирующие сотрудников образовательных организаций.

**3 учебный вопрос** (10 мин): **Рекомендации по использованию социальных медиа-ресурсов сети Интернет должностными лицами Вооруженных Сил Российской Федерации**

Предотвращение возникновения предпосылок утечки информации ограниченного доступа предполагает соблюдение сотрудниками образовательной организации программно-технических и морально-этических принципов использования социальных медиа-ресурсов сети Интернет.

К программно-техническим принципам использования социальных медиа-ресурсов сети Интернет относятся:

- настройка свойств безопасности аккаунтов в социальных медиаресурсах сети Интернет, ограничивающих общий доступ к ним;

- проверка настройки свойств безопасности аккаунтов на предмет ограничения доступа неизвестных пользователей к просмотру персональной информации в аккаунтах социальных медиа-ресурсов сети Интернет сотрудниками образовательной организации;

- установка и регулярное обновление антивирусного и антишпионского программного обеспечения на персональных компьютерах и мобильных устройствах;

- осуществление мониторинга контента персональной страницы на предмет выявления действий посторонних лиц, а, в случае взлома персональной страницы, проведение анализа причины и незамедлительная смена паролей доступа к аккаунту;

- принятие мер по исключению возможности использования своего аккаунта в социальных медиа-ресурсах сети Интернет третьими лицами;

- установка сложных паролей (длиной не менее 14 символов, включая буквы разных регистров и цифры), не совпадающих с паролями к другим сервисам и не состоящих из словарных слов на любом языке, слов в обратном порядке, известных сокращений, повторов букв или их последовательности, а также персональных данных (даты рождения, имена детей и др.);

- обеспечение сохранности паролей в тайне от посторонних лиц, воздержание от использования социальных медиа-ресурсов при подключении к общественным беспроводным сетям и т.д.;

- воздержание от запуска приложений и перехода по ссылкам при отсутствии уверенности в их надежности и легитимности;

- воздержание от использования приложений, разработчики которых могут несанкционированно получить доступ к содержимому аккаунта персональной страницы или персональному мобильному устройству;

- воздержание от использования функций географической привязки и указания координатной информации в персональных мобильных устройствах (приложениях, используемых для доступа к социальным медиа-ресурсам сети Интернет);

- воздержание от включения GPS/ГЛОНАСС-модулей в персональных мобильных устройствах при исполнении рабочих обязанностей и размещения в сети Интернет фото-, аудио- и видеоматериалов с координатной информацией и географической привязкой.

К морально-этическим принципам использования социальных медиа-ресурсов сети Интернет относятся:

- соблюдение высокой культуры общения при использовании социальных медиа-ресурсов сети Интернет;

- проявление уважения к обычаям и традициям других народов, различных этнических, социальных групп и конфессий, способствование межнациональному и межконфессиональному согласию;

- соблюдение требований законодательства Российской Федерации, нормативных правовых актов Президента Российской Федерации в области защиты информации; избежание публикации контента двойного толкования; воздержание от размещения материалов, которые могут содержать компрометирующий, клеветнический, оскорбительный, непристойный или угрожающий характер и способствовать подрыву имиджа Министерства образования и государства в целом;

- воздержание от размещения комментариев, направленных на компрометацию и дискредитацию политического руководства государства, руководства, разжигание религиозной и межнациональной ненависти, поддержку расизма, экстремизма, терроризма, порнографии и иной антиобщественной деятельности, высказывание мнений, которые могут быть расценены как официальная позиция Министерства образования, размещение информации, которая может нарушить неприкосновенность частной жизни других лиц и создавать угрозу для безопасности, здоровья, репутации, свободы личности;

- понимание того, что контент, размещенный в социальных медиаресурсах сети Интернет, мгновенно распространяется, навсегда выходит из-под контроля пользователя, его невозможно удалить с серверного оборудования социальных медиа-ресурсов сети Интернет, и он может быть использован недоброжелателями;

- исключение пользования социальными медиа-ресурсами сети Интернет в неадекватном состоянии (раздражительном, гневном, нетрезвом и др.);

- осознание личной ответственности и возможных последствий своих действий в социальных медиа-ресурсах сети Интернет;

- оценка содержания подготовленного к опубликованию контента на предмет наличия информации ограниченного доступа и возможных последствий для собственной безопасности, безопасности коллег;

- осознание последующей ответственности (уголовной, гражданско-правовой, административной, дисциплинарной) за нарушение законодательства Российской Федерации, нормативных правовых актов Президента Российской Федерации в области защиты информации при использовании социальных медиаресурсов сети Интернет;

- исключение пересылки в социальных медиа-ресурсах сети Интернет служебной информации ограниченного доступа, обсуждений служебной

деятельности и служебной переписки в социальных медиа-ресурсах сети Интернет;

- ведение переписки и общение только с людьми, с которыми знакомы в действительности;

- избежание от включения в список друзей в социальных медиа-ресурсах сети Интернет посторонних и подозрительных лиц;

- регулярная проверка через поисковые системы наличие информации о себе, своей семье, а в случае обнаружения таковой - принятие мер по ее удалению;

- воздержание от общения с пользователями социальных медиа-ресурсов сети Интернет (блогов, форумов), провоцирующих к размещению (публикации) информации ограниченного доступа;

- информирование всех членов семьи, а также близких родственников, друзей и знакомых о возможных угрозах и мерах, направленных на предотвращение указанных угроз, при использовании социальных медиаресурсов сети Интернет.

**III. Заключительная часть – 1 мин.**

1. Подвести итоги занятия.

2. Ответить на поставленные вопросы.

## 1.4. Итоги главы 1

В рамках первой главы нашей работы были рассмотрены теоретические аспекты проблемы формирования компетенции в области информационной безопасности среди сотрудников образовательной организации. Опираясь на научные исследования темы компетентностного подхода, были даны определения терминов компетентность, компетенция. Были определены этапы возникновения, становления и развития компетентностного подхода в отечественной системе образования.

После, были рассмотрены теоретические аспекты компетентности сотрудников образовательной организации в области информационной безопасности. В рамках этого раздела были рассмотрены федеральные государственные образовательные стандарты в области педагогического образования. Раскрывая понятие компетентность в информационной безопасности, были приведены основные виды угроз, сетевых атак, а также даны способы защиты от них. Нами были рассмотрены нормативно правовые акты в области информационно безопасности, даны комментарии по их области действия, а также применяемости в образовательной организации.

В следующем разделе, опираясь на проведённую работу с научными источниками и нормативными актами, мы приступили к созданию модели программы формирования компетентности сотрудников в области информационной безопасности в образовательной организации. Для того, чтобы сделать данную программу наиболее адаптированной под требования пользователя, в соответствии с утвержденными квалификационными требованиями было выделено 3 группы сотрудников в образовательной организации. Для профессорско-преподавательского состава были рассмотрены 2 ФГОС: действующий и утративший силу и на основании анализа сделаны предположения о недостаточном уровне сформированности компетенций в области информационной безопасности среди професорско – преподавательского состава. В целях изучения знаний, умений и навыков данной группы сотрудников, применяемых уже непосредственно в процессе работы, нами были рассмотрены квалификационные характеристики к основным должностям профессорско-преподавательского состава образовательной организации. Данный анализ показал, что проблемам информационной безопасности уделено недостаточно много внимания и что в целях приобретения данных компетенций необходимо вносить изменения в образовательную программу как будущих педагогов, так и в образовательные программы дополнительного образования, которые будут применяться уже во время работы в образовательных организациях.

Основываясь на сделанных выводах и исходя из положений регламентирующих и нормативно правовых документов мы пришли к выводу, что проблемам формирования компетенций уделяется недостаточно много времени и в рамках экспериментальной работы на базе ФВУНЦ ВВС «ВВА» в г. Челябинске попробуем выявить реальный уровень компетенций сотрудников образовательной организации.

# ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНАЯ РАБОТА ПО ФОРМИРОВАНИЮ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДИ СОТРУДНИКОВ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

## 2.1 Организация, цели и задачи эксперимента

Опираясь на выводы, которые были сделаны нами в главе 1, было принято решение провести опрос среди сотрудников образовательной организации, с целью понять реальный уровень компетенций в области информационной безопасности. В рамках этой работы был разработан опросник, который включал в себя 10 вопросов, которые дадут понимание об уровне компетенций сотрудников разных структурных подразделений в области информационной безопасности.

В нашем опроснике 10 вопросов были заданы так, что предполагали максимально открытый вопрос, не ограничивая анкетируемых. Это предоставило возможность наиболее полно оценить уровень сформированности компетенций. Данные вопросы представлены в таблице 2.

Опросник по информационной безопасности

1. Какие проблемы в области информационной безопасности Вы наблюдаете в образовательной организации?
2. Как Вы понимаете значение термина компетентность?
3. Как Вы понимаете значение термина компетенции (компетенция)?
4. Какие существуют составляющие компетенции?
5. Как, по вашему мнению, формируется компетентность?
6. Какие нормативные акты в области информационной безопасности Вы знаете?
7. Какие антивирусные программы вы знаете? Как часто проводятся проверки с помощью них?
8. Что необходимо сделать, если антивирусная программа во время

проверки обнаружила вредоносный файл?

9. В каких случаях возможно подключение машинных носителей информации без установленных реквизитов к ПК?

10. Как вы считаете, возможна ли манипуляция поведением или сознанием обучающегося с помощью ресурсов сети «Интернет»?

Таб. 2

Вопросы включали в себя:

- понимание значений терминов компетентность, компетенция
- знание нормативно-правовых актов в области информационной безопасности
- оценку умений и прикладных навыков в информационной безопасности
- общую оценку системы информационной безопасности в образовательной организации
- умение распознавать возникающие новые угрозы безопасности

В целях автоматизации и стандартизации сбора данных нами были использованы электронные ресурсы, такие как Google Формы см. рисунок 1.

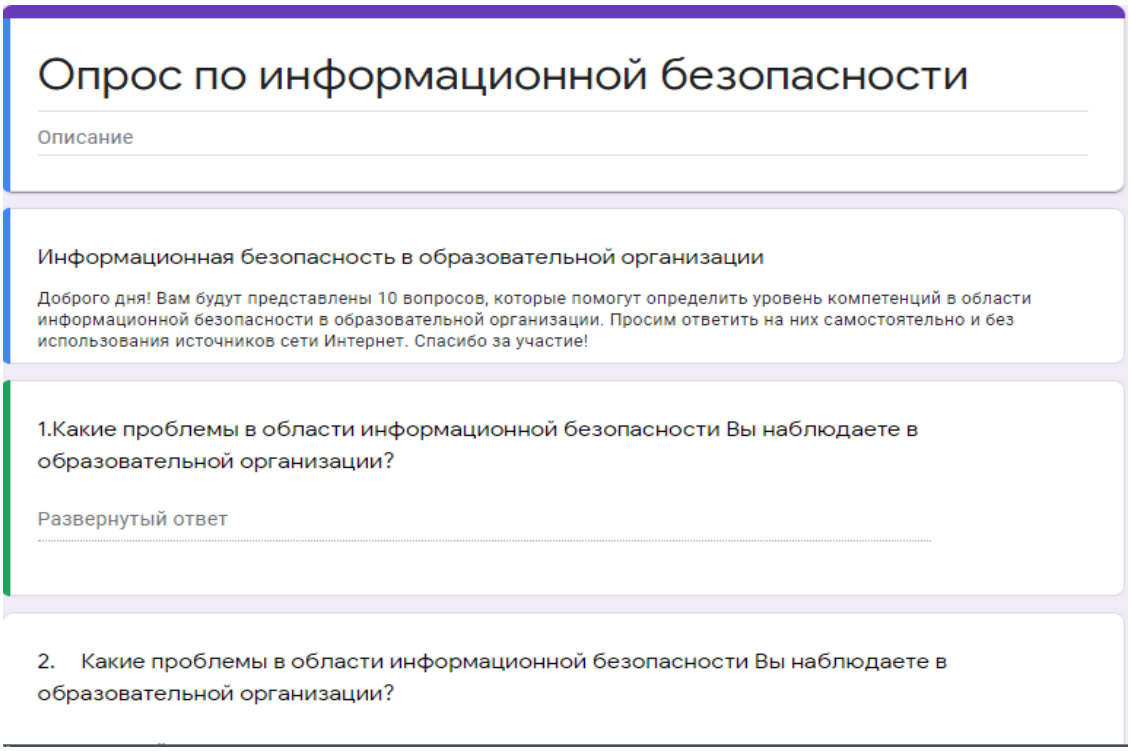


**Рис.1**

К данному опросы были привлечены 2 кафедры образовательного учреждения в составе: 14 сотрудников из числа профессорско-преподавательского состава, 5 сотрудников из числа руководящего состава и 18 сотрудников административно-хозяйственного и учебно-вспомогательного персонала.

При анализе собранных ответов мы разделили опрашиваемых на 3 группы и начали систематизацию ответов. Рассмотрим первыми сотрудников административно-хозяйственного и учебно-вспомогательного корпуса.

На первый вопрос «*Какие проблемы в области информационной безопасности Вы наблюдаете в образовательной организации?»,* ответы разнились. Чаще всего встречались варианты «Недостаточная оснащённость программным обеспечением/персональными компьютерами/средствами защиты информации. Встретилось 2 ответа, что проблем в области информационной безопасности не наблюдается. Вышеупомянутые ответы свидетельствуют о том, что сотрудники данной сферы в большинстве своём анализируют область информационной безопасности и делают выводы о её слабых местах. Вопросам педагогики и обучения не уделено было внимания в ответах, что предположительно связано с отсутствием педагогической работы со студентами.

На второй вопрос «*Как Вы понимаете значение термина компетентность?»* ответы разошлись. Например: достойный уровень знаний человека в определённой области, позволяющий эффективно решать задачи, и наличие навыков в эффективной области для эффективной деятельности, или умение человека хорошо или плохо выполнять свои обязанности и прочее. Отталкиваясь от данного нами определения компетентности в главе 1.1: «Компетентность – владение, обладание человеком соответствующей компетенцией, включающей его личностное отношение к ней и предмету деятельности.», можно сделать выводы, что эта группа сотрудников, достаточно близко изложила значения термина

компетентность, в своём ответе уже пробуя раскрыть значения термина «компетентность».

Третий вопрос звучал «*Как Вы понимаете значение термина компетенции (компетенция)?*» начал вызывать у опрашиваемых сомнение и некую неуверенность в ответе. Так как вопросы 2 и 3 созвучны, опрашиваемые сотрудники пытались разграничить эти 2 понятия. В материалах опросов, которые сданы в бумажном виде были видны исправления в 2,3,4 вопросе, предположительно из желания их разделить и дать наиболее правильное определение каждого из них. Помимо вышеуказанных особенностей стали встречаться прочерки на месте ответа, либо ответ «не знаю» среди 4 сотрудников административно-хозяйственного и учебно-вспомогательного персонала (приблизительно 20%).Наиболее характерными ответами были: способность специалиста решать определенный круг задач, или умения в каком либо вопросе. Также встречались ответы: для меня компетенция и компетентность это одно и то же.

Четвертый вопрос звучал как «*Какие существуют составляющие компетенции?»* и предполагал условно правильным ответ: совокупность взаимосвязанных качеств личности (знаний, умений, навыков, способов деятельности), задаваемых по отношению к определенному кругу предметов и процессов и необходимых для качественной продуктивной деятельности по отношению к ним. Преобладающим ответом были «знания, навыки, опыт, или знания, умения, практика», также встречались ответы «умение применять как практические, так и теоретические навыки». Также встречались и ответы «не знаю», либо «-». Как отмечалось ранее, для сотрудника, не имеющего профильного педагогического образования довольно непросто найти разницу в подобных понятиях, что вызывает повышенный процент отказов от ответа.

Ответы на пятый вопрос « *Как, по вашему мнению, формируется компетентность?*» можно разделить на несколько типовых групп. Первой

группе характерны развёрнутые ответы , как например: компетентность формируется постоянной воспитательной работой и повышением знаний в области обязанностей. Вторая же группа использует ответ на вопрос 4 и дополняет его, например: формируется в совокупности полученных знаний, приобретенных умений в той или иной сфере и применение этих знаний на практике.

Шестой вопрос звучал как «*Какие нормативные акты в области информационной безопасности Вы знаете?*» и ответы опрашиваемых стали гораздо более полными. Звучали следующие ответы: Федеральные законы о коммерческой тайне, о персональных данных. Некоторые опрашиваемые упоминали федеральные законы о информации, информационных технологиях и защите информации. Но большинство ответов содержало отсылки к локальным нормативным актам, таким как инструкция о защите информации от несанкционированного доступа, локальная инструкция по защите информации от несанкционированного доступа на средствах вычислительной техники учебного заведения. Основываясь на ответах опрашиваемых можно сказать, что знания нормативно-правовых актов оцениваются на «хорошо».

Седьмой вопрос звучал «*Какие антивирусные программы вы знаете? Как часто проводятся проверки с помощью них?*» и на него ответили все без исключения респонденты из данной группы. Наиболее часто встречающимися ответами были: Касперский, Dr Web.Также встречались ответы: Авира, Аваст, панда. Опрашиваемые пользуются средствами антивирусной защиты как на рабочем месте, так и на домашних персональных компьютерах. На второй под вопрос респонденты отвечали реже, а также встречались оценочные ответы, такие как «часто», либо «не часто». Чуть больше четверти опрашиваемых ответили « минимум раз в неделю», что соответствует требованиям нормативных документов, принятых в учебном заведении.

Восьмым вопросом был «*Что необходимо сделать, если антивирусная программа во время проверки обнаружила вредоносный файл?*» и на него сотрудники данной группы отвечали согласно алгоритма, утверждённого памятками и инструкциями по информационной безопасности. Более 75% опрошенных ответили, что необходимо оповестить сотрудников подразделения информационной безопасности, а не пытаться исследовать или как то иначе взаимодействовать с вредоносным файлом. Данный ответ соответствует типовому алгоритму действий при обнаружении вирусного программного обеспечения, описанному в инструкциях, утверждённых в образовательной организации.

Девятый вопрос звучал как «*В каких случаях возможно подключение машинных носителей информации без установленных реквизитов к ПК?*» и подразумевал под собой ситуацию, когда к средству вычислительной техники, зарегистрированному установленным порядком пытаются подключить машинный носитель информации (например USB – флеш, оптический диск, карту памяти) без нанесённых на неё реквизитов о регистрации. Данная ситуация является несанкционированным доступом к информации и не должно допускаться при работе на средствах вычислительной техники согласно введённых в действие инструкций. Лишь четверть респондентов ответили на это вопрос правильно, остальные же написали, что такое подключение возможно, либо затруднились дать ответ.

Десятый вопрос звучал как «*Как вы считаете, возможна ли манипуляция поведением или сознанием обучающегося с помощью ресурсов сети «Интернет»*» и выходил за привычные рамки оценки информационной безопасности. Подобный вопрос не рассматривается в инструкциях по защите информации и подразумевает умение респондентов критически мыслить, принимать правильные решения в нестандартных ситуациях. Ответы опрашиваемых разнились от «Да», «Возможно» до категоричных «Нет». Был небольшой процент опрашиваемых, который пытался в своём ответе опираться на обучение студентов и преломить манипуляцию

поведением и сознанием на обучаемых. Если проанализировать уровень компетентности сотрудников административно-хозяйственного и учебно-вспомогательного персонала в данном вопросе, то можно сказать, что он недостаточен для умелого противостояния новым возникающим угрозам.

Подводя промежуточный итог по ответам опрашиваемых сотрудников административно-хозяйственного и учебно-вспомогательного корпуса, можно выделить некоторые характерные особенности. Вопросы 2-5 вызывали у данной группы респондентов наибольшие затруднения, что объясняется их спецификой работы и профильным образованием, которое не включало в себя изучение компетентностного подхода. В то же время, вопросы 6-8 были наиболее простыми, а ответы на них были наиболее правильными. Это объясняется тем, что в большинстве своём вопросами защиты информации на факультетах и кафедрах занимаются сотрудники административно-хозяйственного и учебно-вспомогательного корпуса, приобретая в процессе данной работы устойчивые практические навыки в данной области, а также знания основных регламентирующих документов.

Следует также выделить 2 последние вопроса, которые вызвали затруднение и неоднозначные ответы среди респондентов. На вопросы несанкционированного доступа с связанных с угрозами исходящими от неучтённых носителей информации, а также на вопросы безопасности в социальных- медиа ресурсах требуется уделить наибольшее внимание.

Второй группой опрашиваемых были представители руководящего состава образовательной организации, в количестве 5 человек. Даже при поверхностном анализе было видно, что их ответы сильно отличались от сотрудников административно-хозяйственного и учебно-вспомогательного корпуса. Рассмотрим ответы подробнее.

На первый вопрос «*Какие проблемы в области информационной безопасности Вы наблюдаете в образовательной организации?*» типовым ответом был «низкая образованность в этом вопросе исполнителей», либо «малое количество занятий на тему информационной безопасности».

Становится очевидно, что руководители на первое место ставят компетенции своих подчинённых сотрудников.

Анализируя ответы на второй вопрос «*Как Вы понимаете значение термина компетентность?»* среди руководящего состава, частыми были ответы на подобие «способность должностных лиц выполнять свои обязанности на высоком профессиональном уровне». После двух вопросов у группы респондентов ярко прослеживается их руководящая должность, так как все ответы нацелены на подчинённые подразделения и формирование в первую очередь их компетенций.

Третий вопрос «*Как Вы понимаете значение термина компетенции (компетенция)?»* лишь подтвердил гипотезу, высказанную выше. Ответы были направлены на подчинённые подразделения и звучали как «То. Чем должностные лица должны владеть в совершенстве», либо «умение выполнить ту или иную функциональную обязанность».

На четвертый вопрос « *Какие существуют составляющие компетенции?*» группа респондентов чаще всего отвечала «знания, опыт», либо «знать, уметь, владеть». Стоит отметить, что в группе руководящего состава принимали участие руководители различных структурных подразделений, в том числе и не связанных напрямую с образовательной деятельностью, а административно хозяйственных и учебно вспомогательных. Данный факт может объяснить то, что вопросам компетенций, их формирования уделено мало влияния со стороны опрашиваемых. На первый план группа руководящего состава ставит исполнение непосредственных функциональных обязанностей, тем самым ставя на второй план процесс формирования компетенций, не относящихся напрямую к исполнению рабочих функций.

Пятый вопрос « *Как, по вашему мнению, формируется компетентность?*» вызвал различные ответы, такие, как например «упорным выполнением должностных обязанностей», «дополнительной подготовкой должностных лиц». Так как вопрос был открытым и не

ставилось никаких ограничений, связанных с ответом, встретились ответы и с юмором, как например «с потом, кровью, слезами…». Если проанализировать данные ответы, можно понять, что наша гипотеза о ярко выраженной роли руководителя всё крепнет, так как во главу угла ставится упорное выполнение должностными лицами своих функциональных обязанностей.

Шестой вопрос «*Какие нормативные акты в области информационной безопасности Вы знаете?*» поделил группу на 2 части. 3 участника перечислили довольно большой список законов, нормативных актов и локальных инструкций, связанных с обеспечением информационной безопасности. Вторая подгруппа, из 2 человек ушла от ответа, написав что то похожее на «слишком много, чтобы перечислять».

Ответы на седьмой вопрос « *Какие антивирусные программы вы знаете? Как часто проводятся проверки с помощью них?*» были логическим продолжением предыдущих и звучали как «те, которые рекомендованы к установке», либо «программы, как решат в руководящих документах».

На восьмой вопрос «*Что необходимо сделать, если антивирусная программа во время проверки обнаружила вредоносный файл?»* группа опрашиваемых ответила про ответственность должностного лица за данное заражение средства вычислительной техники. Звучали ответы «наказать должностных лиц, причастных», либо «провести разбирательство и наказать виновных».

Девятый вопрос звучал как «*В каких случаях возможно подключение машинных носителей информации без установленных реквизитов к ПК?*» и давал меньше возможностей для трактовки его в руководящем русле. Звучали ответы «Запрещено», «Ни в каких», что соответствует требованиям руководящих документов и инструкций. Данные ответы дают понять, что группа опрашиваемых из руководящего состава обладает необходимыми компетенциями и респонденты смогли ответить на данный вопрос верно.

На десятый вопрос «*Как вы считаете, возможна ли манипуляция поведением или сознанием обучающегося с помощью ресурсов сети «Интернет»»* ответы группы опрашиваемых были положительными. Представители руководящего состава осознают опасность от данного вида угроз и задумываются о формировании у подчинённых должностных лиц компетенций для противодействия им.

Подводя итог по второй группе опрашиваемых, очевидна модель поведения и мысли группы руководителей. Даже на отдалённые от основной деятельности вопросы они отвечали исходя в первую очередь из обязанностей своих и своих структурных подразделений. Что касается компетенций в подчинённых структурных подразделений в области информационной безопасности – он поддерживается на минимально необходимом уровне, в основном за счёт знания внутренних руководящих документов и умения ими пользоваться.

Завершающей, третьей группой опрашиваемых были 14 представителей профессорско-преподавательского состава. Даже при беглом анализе ответов на вопросы третьей группы стало видно, что ответы гораздо более полные, в них всесторонне раскрыты вопросы и донесена суть. Рассмотрим их подробнее.

Первый вопрос «*Какие проблемы в области информационной безопасности Вы наблюдаете в образовательной организации?*» вызвал в большинстве своём развёрнутые ответы с описанием недостатков. Большинство из них были применимы к процессу обучения студентов, но один из ответов заслуживает особого внимания, так как он представляет анализ как системы информационной безопасности, так и мер по формированию компетенций в области информационной безопасности. Преподаватель пишет: « В области информационной безопасности в образовательной организации есть ряд проблем, одна из которых – это слабые навыки и знания у пользователей ПК. Следующая проблема – это отсутствие конкретики в области разрешённого программного обеспечения.

Ещё одна проблема – это отсутствие четких и понятных правил в области информационной безопасности, излишняя громоздкость инструкций и правил». Данный ответ показывает высокий уровень аналитических способностей, так как видно не только умение анализировать проблемы, но и практически предложены готовые решения их. Как мы упоминали ранее, данный ответ, как и большинство ответов группы профессорско преподавательского состава направлен на процесс обучения, так как поднимается проблема облегчения восприятия сложных требований из инструкций и адаптации для людей – не специалистов.

Ответы на второй вопрос «*Как Вы понимаете значение термина компетентность?*» приятно порадовали высоким знанием со стороны профессорско-преподавательского состава. Почти все ответы были комплексными, включали в себя следующее: « Компетентность – комплекс знаний, умений и навыков в определённой области», что соответствует в общих чертах определению, данному нами ранее, в главе 1.1.

Ответы на третий вопрос «*Как Вы понимаете значение термина компетенции (компетенция)?*» также у большинства респондентов содержал отсылки к знаниям, умениям и навыкам. Встречались ответы «совокупность знаний, умений и навыков, относящаяся к определённой области».

Четвертый вопрос «*Какие существуют составляющие компетенции?*» также содержал в себе отсылки к «знаниевому» подходу. Более 60% опрашиваемых ответили, что компетенции состоят из знаний, умений и навыков

Пятый вопрос «*Как, по вашему мнению, формируется компетентность?*», оказался более творческим, а ответы на него более развёрнутыми. Примечателен ответ одного из респондентов: «компетентность формируется в ходе образовательного процесса. Сначала поступают знания в виде информации, затем в ходе практических занятий вырабатываются умения. По выпуску, а также в ходе различных тренингов

формируется компетентность». На наш взгляд это наиболее полный ответ на данный вопрос, среди всех представленных.

Шестой вопрос *«Какие нормативные акты в области информационной безопасности Вы знаете?»* не вызвал затруднения у группы опрашиваемых. Практически все назвали инструкции по защите информации, которые утверждены соответствующими распоряжениями, в пределах образовательной организации. Но в то же время, лишь 20% респондентов называли федеральные законы и иные нормативные акты, которые действуют и вне образовательной организации.

Ответы на седьмой вопрос «*Какие антивирусные программы вы знаете? Как часто проводятся проверки с помощью них?*» в основном сводились к перечислению списка программ, используемых в образовательной организации. Лишь 5 участников опроса из группы профессорско-преподавательского состава указали антивирусные программы, не входящие в список рекомендуемых к установке. Касаемо частоты проверок антивирусными средствами, ответы в большинстве были правильными и соответствовали требованиям локальных нормативных документов, но в то же время, лишь 3 ответа полностью соответствовали всем требованиям к антивирусным проверкам.

На восьмой вопрос «*Что необходимо сделать, если антивирусная программа во время проверки обнаружила вредоносный файл?*» также не было неверных ответов. Все респонденты группы ответили, что необходимо незамедлительно сообщить в подразделение информационной безопасности и действовать по их указаниям, что соответствует требованиям локальных актов.

Девятый вопрос «*В каких случаях возможно подключение машинных носителей информации без установленных реквизитов к ПК?*» также не вызвал затруднения среди профессорско – преподавательского состава. Все участники этой группы правильно оценили данный кейс на соответствие

требованиям информационной безопасности и верно ответили, что подключение запрещено.

На десятый вопрос «*Как вы считаете, возможна ли манипуляция поведением или сознанием обучающегося с помощью ресурсов сети «Интернет»?»* ответы разделились. 7 респондентов считали, что такое воздействие посредством сети интернет возможно. 4 участника опроса ответили, что таких манипуляций быть не может. 3 участника ответили утвердительно, но с некоторыми особенностями. Приведу пример одного из этих ответов «Управление сознанием только через сеть интернет невозможно, могут быть «лазейки», связанные с личной неосторожностью, афишированием своей жизни в социальных сетях».

*Подводя итоги* экспериментальной работе по опросу сотрудников образовательной организации, выделяются следующие особенности, которые будут учтены при разработке методики формирования компетенции в области информационной безопасности.

Так, в теоретической части нашей работы сотрудники были поделены на 3 различные группы по направлениям деятельности: профессорско-преподавательский состав, руководящий состав, сотрудники административно-хозяйственного и учебно-вспомогательного персонала. Во время опроса трёх групп были выявлены сильные различия среди опрашиваемых, связанные с их профессиональной деятельности. Подытожим особенности каждой из групп.

Ответы группы сотрудников административно-хозяйственного и учебно-вспомогательного персонала характеризуются невысокими знаниями терминов компетентность, компетенция и основных положений компетентностного подхода. В то же время, знания и практические навыки группы сотрудников оцениваются как хорошие, по результатам ответов на вопросы на практические вопросы. Это в большинстве случаев обусловлено тем, что практическими аспектами обеспечения информационной безопасности заняты на кафедрах именно эти сотрудники. Основные

положения, на которые стоит обратить внимание в подготовке сотрудников административно-хозяйственного и учебно-вспомогательного корпуса – организационная защита информации в учебном заведении и безопасность в социальных медиа-ресурсах.

Ответы группы руководящего состава даёт ясную картину о роли их в жизни коллектива и процессе формирования компетенций сотрудников в области информационной безопасности. На вопросы 2-5 респонденты из 2 группы отвечали не верно, не стремясь вникнуть в суть. Следующие вопросы касались конкретных компетенций в упомянутой области и ответы группы опрашиваемых показали минимально необходимый уровень. Очевидно, что для данной группы необходимо включить в курс повышения их компетенций сведения об актуальных угрозах информационной безопасности, возможности их реализации и возможных последствиях, так как данным вопросам уделяется лишь второстепенное значение.

Ответы группы профессорско-преподавательского состава порадовали высоким знанием терминов «компетентность», «компетенция», общим пониманием компетентностного подхода в образовании. Следующие вопросы показали знания нормативно-правовой базы на уровне выше среднего, всеми опрашиваемыми были названы основные регламентирующие внутренние документы. Практические навыки опрашиваемой группы были на уровне, позволяющем обеспечить безопасное функционирование средств вычислительной техники, а также безопасное обучение студентов. Последний, десятый вопрос разделил ответы среди группы профессорско – преподавательского состава поэтому нельзя с уверенностью сказать, что данная группа сотрудников готова противостоять возникающим новым угрозам информационной безопасности, в первую очередь исходящим из сети Интернет.

## 2.2 Внедрение технологий формирования компетенции

Опираясь на выводы, сделанные нами ранее, результаты анкетировании группы сотрудников образовательной организации, было принято решение проанализировать систему дополнительного обучения сотрудников образовательной организации.

В рассматриваемой образовательной организации процесс повышения квалификаций организован в соответствии с законодательством Российской Федерации, а также в соответствии с локальными нормативными актами. Профессорско – преподавательский состав, в соответствии с ч. 2 п. 5 ст. 47 Федерального закона от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации", имеет право на дополнительное профессиональное образование по профилю педагогической деятельности не реже чем один раз в три года.

Также, не реже чем раз в неделю проводятся занятия, на которых доводятся основные требования законодательства, проводится информирование всех категорий сотрудников. Не реже чем раз в квартал проводятся доведения основных требований основных нормативных актов в области информационной безопасности, а также лекции с теоретической информацией об угрозах и информацией о наказании лиц виновных в реализации этих угроз.

Опираясь на сформировавшуюся систему получения дополнительных знаний, а также в рамках следующего этапа экспериментальной работы по формированию компетенций было принято решение в рамках профессиональной подготовки провести серию дополнительных занятий, как лекционных, так и практических. В данном эксперименте приняли участие сотрудники 2 кафедр, которые ранее принимали участие в анкетировании. При планировании дополнительных занятий был учтён опыт анкетирования, сфера деятельности групп работников.

Подытоживая констатирующую часть нашей экспериментальной работы, были сделаны выводы об уровне сформированности компетенций

различных групп сотрудников. Результаты данной работы представлены в таблице 3.

| Наименование группы сотрудников | Область знаний, где показаны наихудшие результаты | Область знаний, где показаны наилучшие результаты |
|---|---|---|
| Руководящий состав | -слабые практические навыки<br>-придают второстепенное значение вопросам информационной безопасности | -знание нормативных документов |
| Профессорско-преподавательский состав | -безопасность в социальных медиа-ресурсах | -понятийный аппарат компетентностного подхода<br>-знания нормативно-правовой базы<br>-практические навыки антивирусной защиты |
| Административно-хозяйственный и учебно-вспомогательный персонал | -низкий уровень знаний о компетентностном подходе<br>-слабые знания об угрозах в социальных медиа-ресурсах<br>-организационная защита информации | -устойчивые практические навыки |

Таблица 3

Опираясь на эти выводы были спланированы 3 разных курса для повышения компетенций разных групп должностных лиц, опираясь на сильные стороны и дополняя слабые.

Так, для группы руководящего состава в перечень тем для изучения вошли «Угрозы информационной безопасности и последствия их реализации», а также практическое занятие «Система защиты информации на рабочем месте. Методы настройки и порядок работы с ней». Опираясь на высокое знание группой руководителей нормативной базы, в лекционном занятии будет уделено особое внимание вопросам ответственности за нарушения данной направленности. В состав практического занятия войдут занятия с использованием нескольких средств вычислительной техники. Опираясь на требование методик настройки средств защиты информации, глядя на пример, который выводится на мультимедийный экран изображение рабочего стола лектора, группа обучаемых сможет пошагово настроить систему защиты информации на средстве вычислительной техники. Данные навыки пригодятся для самоконтроля, а также для контроля подчинённых в соответствии с требованиями руководящих документов.

Для группы административно-хозяйственного и учебно-вспомогательного персонала были спланированы для проведения лекционные занятия по темам: «Организационная защита информации. Структура системы защиты, основные направления», «Угрозы безопасности информации в социальных медиа ресурсах». Для группы, обладающей устойчивыми навыками в настройке средств защиты информации важно получить общее понимание системы защиты информации в образовательном учреждении, возможные угрозы а также способы им противостоять.

Группа профессорско – преподавательского состава показала наивысший уровень сформированности компетенций в области информационной безопасности. Для повышения их компетенций были выбраны следующие лекционные занятия: «Угрозы безопасности информации в социальных медиа ресурсах», «Угрозы информационной

безопасности и последствия их реализации». Данный курс лекций позволит группе получить знания о нестандартных угрозах безопасности, чтобы уметь противостоять их реализации.

Данный курс выстраивался, применяя методы личностно-ориентированного подхода. При формировании тем, в дальнейшем, во время лекционных и практических занятий учитывались сильные стороны и темы были подобраны таким образом, чтобы сильные стороны знаний и умений обучаемых помогали в формировании слабых.

Все занятия по указанным темам проводились в рамках профессиональной подготовки. Рассмотрим организацию курса подготовки на примере группы сотрудников административно-хозяйственного и учебно-вспомогательного корпуса. Нами было проведено 2 лекционных занятия, с промежутком в неделю на которых обучаемые слушали лектора и делали конспекты. Опираясь на сборник конспектов лекций Н.В. Ясенева нами были разработаны 2 план-конспекта занятий с данной группой сотрудников.

**ПЛАН – КОНСПЕКТ**

**проведения занятия с сотрудниками административно-хозяйственного и учебно-вспомогательного персонала**

**Время проведения:** 20 мин

**Место проведения:** конференц-зал

**Материальное обеспечение:**

1. Мультимедийная аппаратура (слайдовая презентация).

**ХОД ЗАНЯТИЯ**

**I. Вводная часть – 1 мин.**

1. Проверить наличие обучаемых.
2. Объявить тему и цель занятия, время и порядок проведения.
3. Вступление.

Основными задачами организационной защиты информации является регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

**II. Основная часть – 18 мин.**

**1 учебный вопрос (**10 мин): **Организационно-техническое обеспечение компьютерной безопасности**

Организационное обеспечение – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий.

Организационное обеспечение компьютерной безопасности включает в себя ряд мероприятий:

организационно-административные; организационно-технические; организационно-экономические.

Организационно-административные мероприятия предполагают:

минимизацию утечки информации через персонал (организация мероприятий по подбору и расстановке кадров, создание благоприятного климата в коллективе и т. д.);

организацию специального делопроизводства и документооборота для конфиденциальной информации, устанавливающих порядок подготовки, использования, хранения, уничтожения и учета документированной информации на любых видах носителей;

выделение специальных защищенных помещений для размещения средств вычислительной техники и связи, а также хранения носителей информации;

выделение специальных средств компьютерной техники для обработки конфиденциальной информации;

организацию хранения конфиденциальной информации на промаркированных отчуждаемых носителях в специально отведенных для этой цели местах;

использование в работе сертифицированных технических и программных средств, установленных в аттестованных помещениях; организацию регламентированного доступа пользователей к работе со средствами компьютерной техники, связи и в хранилище (архив) носителей конфиденциальной информации;

установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

контроль соблюдения требований по защите конфиденциальной информации.

Система организационных мероприятий, направленных на максимальное предотвращение утечки информации через персонал включает:

оценка у претендентов на вакантные должности при подборе кадров таких личностных качеств, как порядочность, надежность, честность и т. д.;

ограничение круга лиц, допускаемых к конфиденциальной информации; проверка надежности сотрудников, допускаемых к конфиденциальной

информации, письменное оформление допуска; развитие и поддержание у работников компании корпоративного духа,

создание внутренней среды, способствующей проявлению у сотрудников чувства принадлежности к своей организации, позитивного отношения человека к организации в целом (лояльность);

проведение инструктажа работников, участвующих в мероприятиях, непосредственно относящихся к одному из возможных каналов утечки информации.

Все лица, принимаемые на работу, проходят инструктаж и знакомятся с памяткой о сохранении служебной или коммерческой тайны. Памятка разрабатывается системой безопасности с учетом специфики организации.

Сотрудник, получивший доступ к конфиденциальной информации, подписывает индивидуальное письменное обязательство об ее неразглашении. Обязательство составляется в одном экземпляре и храниться в личном деле сотрудника не менее 5 лет после его увольнения. При увольнении из организации сотрудником дается подписка. Функции отобрания обязательства и подписок возлагаются на кадровый аппарат организации.

Служащий организации, подписывая подобного рода документ, должен четко представлять, что конкретно из конфиденциальной информации является тайной организации. В том числе по этой причине необходимо, чтобы вся конфиденциальная информация была обособлена от остальных сведений, а документы, ее содержащие, носили соответствующий гриф.

Использование обязательств о сохранении конфиденциальной информации позволяет обеспечить ее юридическую защиту, к которой имеет (или имел) доступ персонал организации.

Все руководители, сотрудники и технический персонал должны быть охвачены регулярной подготовкой по вопросам обеспечения информационной безопасности. При этом должно быть два вида обучения: первоначальное и систематическое.

С увольняющимися сотрудниками проводятся беседы, направленные на предотвращение разглашения конфиденциальной информации. Эти обязательства, как правило, подкрепляются соответствующей подпиской.

Организацией конфиденциального делопроизводства является:

– документирование информации;

– учет документов и организация документооборота;

– обеспечение надежного хранения документов;

– проверка наличия, своевременности и правильности их исполнения;

– своевременное уничтожение документов.

**2 учебный вопрос (**8 мин): **Структура системы защиты, основные направления.**

Для обеспечения эффективности защиты информации все используемые средства и мероприятия целесообразно объединить в систему защиты информации, которая должна быть функционально самостоятельной подсистемой ИС. Главное свойство системы защиты – адаптивность ее при изменении структуры технологических схем или условий функционирования ИС. Другими принципами могут быть:

минимизация затрат, максимальное использование серийных средств;

обеспечение решения требуемой совокупности задач защиты;

комплексное использование средств защиты, оптимизация архитектуры;

удобство для персонала;

простота эксплуатации.

Систему защиты информации целесообразно строить в виде взаимосвязанных подсистем: криптографической защиты; обеспечения юридической значимости электронных документов; защиты от несанкционированного доступа (НСД); организационно-правовой защиты; управления системой защиты информации (СЗИ).

Построение системы защиты информации в таком виде позволит обеспечить комплексность процесса защиты информации в ИС,

управляемость процесса и возможность адаптации при изменении условий функционирования ИС.

Подсистема криптографической защитыобъединяет средства такой защиты информации и по ряду функций кооперируется с подсистемой защиты от НСД.

Подсистема обеспечения юридической значимости электронных документовслужит для придания юридического статуса документам в электронном представлении и является определяющим моментом при переходе к безбумажной технологии документооборота. Данную подсистему удобно и целесообразно рассматривать как часть подсистемы криптографической защиты.

Подсистема защиты от НСД предотвращает доступ несанкционированных пользователей к ресурсам ИС.

Подсистема управления СЗИ предназначена для управления ключевыми структурами подсистемы криптографической защиты, а также контроля и диагностирования программно-аппаратных средств и обеспечения взаимодействия всех подсистем СЗИ.

Подсистема организационно-правовой защитыпредназначена для регламентации деятельности пользователей ИС и представляет собой упорядоченную совокупность организационных решений, нормативов, законов и правил, определяющих общую организацию работ по защите информации в ИС.

Стандарты безопасности Документы Государственной технической комиссии России

В 1992 г. Гостехкомиссия (ГТК) при Президенте Российской Федерации разработала и опубликовала пять руководящих документов, посвященных вопросам защиты информации в автоматизированных системах ее обработки.

Основой этих документов является концепция защиты средств вычислительной техники от несанкционированного доступа к информации,

содержащая систему взглядов ГТК на проблему информационной безопасности и основные принципы защиты компьютерных систем. С точки зрения разработчиков данных документов, основная задача средств безопасности – это обеспечение защиты от несанкционированного доступа к информации.

Определенный уклон в сторону поддержания секретности информации объясняется тем, что эти документы были разработаны в расчете на применение в информационных системах силовых структур РФ.

Руководящие документы ГТК предлагают две группы требований к безопасности – показатели защищенности средств вычислительной техники (СВТ) от НСД и критерии защищенности автоматизированных систем (АС) обработки данных. Первая группа позволяет оценить степень защищенности отдельно поставляемых потребителю компонентов КС, а вторая рассчитана на более сложные комплексы, включающие несколько единиц СВТ.

Показатели защищенности средств вычислительной техники от несанкционированного доступа

Данный руководящий документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Данные показатели содержат требования защищенности СВТ от НСД к информации и применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ).

Важно отметить, что требования являются классическим примером применения необходимых условий оценки качества защиты, т.е. если какой-либо механизм присутствует, то это является основанием для отнесения СВТ к некоторому классу.

Классы защищенности автоматизированных систем (АС)

Документы ГТК устанавливают девять классов защищенности АС от НСД, каждый из которых характеризуется определенной совокупностью требований к средствам защиты. Классы подразделяются на три группы, отличающиеся спецификой обработки информации в АС. Группа АС определяется на основании следующих признаков:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий пользователей АС на доступ к конфиденциальной информации;

режим обработки данных в АС (коллективный или индивидуальный).

В пределах каждой группы соблюдается иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, гдеN– номер группы (от 1 до 3). Следующий класс обозначаетсяNБ и т.д. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой в АС на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности. Не все пользователи имеют равные права доступа. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А. Рассмотренные документы необходимо воспринимать как первую стадию формирования отечественных стандартов в области информационной безопасности.

На разработку этих документов наибольшее влияние оказала «Оранжевая книга», однако это влияние в основном отражается в ориентированности обеих групп документов на защищенные системы силовых структур и в использовании единой универсальной шкалы оценки степени защищенности.

К недостаткам данного стандарта относятся: ориентация на противодействие НСД и отсутствие требований к адекватности реализации политики безопасности. Понятие «политика безопасности» трактуется исключительно как поддержание режима секретности и отсутствие НСД. Из-за этого средства защиты ориентируются исключительно на противодействие внешним угрозам, а к структуре самой системы и ее функционированию не предъявляется четких требований.

Ранжирование требований по классам защищенности по сравнению с остальными стандартами информационной безопасности максимально упрощено и сведено до определения наличия или отсутствия заданного набора механизмов защиты, что существенно снижает гибкость требований и возможность их практического применения.

Несмотря на указанные недостатки, документы ГТК заполнили «правовой вакуум» в области стандартов информационной безопасности в России и оперативно решили проблему проектирования и оценки качества защищенных КС.

**III. Заключительная часть – 1 мин.**

1. Подвести итоги занятия.

2. Ответить на поставленные вопросы.

Также, во время лекционного курса, группа сотрудников административно-хозяйственного и учебно-вспомогательного корпуса прослушала лекцию об угрозах в социальных медиа-ресурсах, которая была приведена в главе 1.3. 2 лекционных занятия прошли успешно, после них были заданы вопросы, которые были призваны раскрыть тему ещё глубже, дать ответы на вопросы, которые назрели у группы обучаемых ещё раньше.

В процессе работы с группой обучаемых складывалось впечатление, что данные сотрудники всё глубже разбираются в вопросах информационной безопасности, уровень компетентности в данных вопросах повышается.

Данную гипотезу мы проверим в дальнейшем, способом повторного анкетирования.

2 других группы обучаемых также прошли курс из лекций, а также практических занятий. Стоит отметить, что характерные для каждой из групп особенности оставались на протяжении всего периода дополнительного обучения.

Так, в период обучения группы руководящего состава наблюдалась модель поведения, которую образно можно назвать «руководитель». На начальном этапе высказывались сомнения в целесообразности этих знаний, были озвучены мысли, что знаниями в информационной безопасности должны обладать сотрудники подразделений по защите информации. Данные сомнения перестали озвучиваться после доведения информации о практике реализации угроз информационной безопасности, об ущербе, который они наносят. Особенно вдумчиво была воспринята информация, касающаяся наказаний за нарушения требований нормативных документов в области информационной безопасности. После двух указанных лекционных занятий, практическое занятие прошло более сосредоточенно.

Группа профессорско – преподавательского состава, ожидаемо хорошо восприняла лекционные занятия, повысила свой уровень знаний в области информационной безопасности. По вопросам, которые задавались после лекционного занятия по теме «Информационная безопасность в социальных медиа-ресурсах» было понятно, что эта группа обучаемых активно познаёт вновь возникающие угрозы в области информационной безопасности, а также ищет ответы на свои вопросы.

*Подводя итоги* параграфа хотелось бы отметить, что опираясь на обратную связь (вопросы после лекционных и во время практических занятий), можно предположить, что уровень сформированности компетентности всех категорий сотрудников образовательной организации растёт. Данное утверждение мы проверим в следующей главе.

Практическое реализации курса лекционных и практических занятий заняло около 2 недель и содержало 2 лекционных занятия, 1 практическое. Учитывая специфику образовательной организации, в которой проводилось исследование и опираясь на положения пункта 1.1 статьи 7 Федерального закона «О статусе военнослужащих»[80], нам было запрещено проводить фотографическую фиксацию процесса эксперимента, а также открыто опубликовывать его результаты.

## 2.3 Результаты экспериментальной работы

После проведённой созидательно – преобразующей части нашего эксперимента, было принято решение проверить прогресс обучающихся групп сотрудников. Так, спустя неделю после завершения занятий по курсу лекций, группы обучаемых были снова опрошены, с целью понять, как изменилась их компетентность в области информационной безопасности.

Чтобы понять изменения компетенций в области информационной безопасности, было принято решение повторить тестирование, которое мы описывали в параграфе 2.1. Решение оставить вопросы теми же было осознанным и обусловлено тем, чтобы сравнение было наиболее корректным, а тот фактор, что обучаемые уже знают, какими будут вопросы компенсируется разницей между опросами более месяца.

Поскольку критериев, объективно и однозначно отвечающих цели исследования, выявлено не было, нами разработаны критериальные показатели, которые служат оценкой сформированности как отдельных компетенций, так и компетентности в ИБ в целом (таблица 3). Эти критерии используются в поэлементном анализе для определения уровня информационной компетентности каждого студента. Опираясь на научные исследования Н.Н. Нагайченко[63] под понятием «критерий» мы понимаем признак, на основании которого производится мониторинг чего-либо, позволяющий произвести измерения предмета и, на основании этого, дать ему оценку.

*Критерии оценивания компетенций в области информационной безопасности среди сотрудников образовательной организации*

| № | Название критерия | Характеристика | Баллы |
|---|---|---|---|
| Практические компетенции | | | |
| 1 | Знание общих принципов функционирования системы защиты информации | Сотрудник обладает знаниями о задачах пользователей, администраторов безопасности, структуре защиты информации и может анализировать эту деятельность | 2 |
| | | Сотрудник знает большую часть своих обязанностей, как пользователя, не знает устройство системы защиты информации в целом. | 1 |
| | | Сотрудник не знаком с системой защиты информации в учебном заведении | 0 |
| 2 | Знание основных регламентирующих документов | Сотрудник знает все обязательные для изучения нормативные акты, знает дополнительные по направлению деятельности | 2 |
| | | Сотрудник знает минимально необходимое количество нормативных документов | 1 |
| | | Сотрудник затрудняется назвать нормативные документы | 0 |
| 3 | Знание антивирусных программ, умение применять их. | Сотрудник знает все программы, рекомендованные к установке, знает периодичность антивирусной проверки | 2 |
| | | Сотрудник называет часть программ, знает периодичность проверки | 1 |
| | | Сотрудник не знает, какие должны использоваться программы, не знает, как часто проводятся проверки | 0 |
| 4 | Знание принципов функционирования программной части средств защиты информации | Сотрудник обладает указанными знаниями, необходимыми для безопасного выполнения задач с помощью персонального компьютера | 2 |
| | | Знания программной части системы ЗИ являются фрагментарными, но достаточными для выполнения служебных задач с помощью ПК | 1 |
| | | Сотрудник не обладает знаниями программной части средств защиты информации, вследствие чего безопасное выполнение задач с помощью ПК невозможно | 0 |

| | | | |
|---|---|---|---|
| 5 | Знание правил регистрации и использования машинных носителей информации в организации | Пользователь знает, как проходит регистрация, знает реквизиты учтенных носителей информации, правильно применяет знания на практике | 2 |
| | | Пользователь не знает реквизиты, но знает, что подключение без них запрещено | 1 |
| | | Пользователь не знает правил подключения носителей информации к служебным ПК | 0 |
| 6 | Знания в области новых угроз (в сети Интернет) | Сотрудник осознаёт, что есть новые, не предусмотренные регламентами угрозы информационной безопасности. Умеет отличать их и осознаёт необходимость с ними бороться. | 2 |
| | | Сотрудник понимает, что в сети интернет есть угрозы безопасности, но знания ограничиваются на простейших угрозах. Не берутся в расчёт угрозы манипуляции и обмана. | 1 |
| | | Сотрудник считает, что в интернете нет угроз | 0 |

Таблица 3.

Так как ответы в опроснике изначально были открытыми и не предполагали правильных и неправильных вариантов ответа, в таблице 3 мы попытались стандартизировать требования к ответам опрашиваемых. Были выделены 3 категории соответствия ответов правильным. Первая – полностью соответствует, ответ раскрывает комплексное знание вопроса, показывает знание и умения опрашиваемого, позволяет решить поставленную учебную задачу. Вторая – частично соответствует, ответ показывает лишь часть знаний о заданном вопросе, допускается, что не упоминаются какие то части. Но в ответе указан правильный путь решения поставленной учебной задачи. Третья – полностью не соответствует, навыки и знания в указанном вопросе у опрашиваемого отсутствуют. Ответ опрашиваемого ведёт к реализации угрозы информационной безопасности.

С помощью таблицы 3 нами были проанализированы практические навыки в области информационной безопасности среди всех 37 участников эксперимента, применимо к ответам на первую часть опроса. Уровень баллов сформированности компетенций был также разделен по 3 категориям

сотрудников. Далее будут приведены средние значения за группу, округлённые по математическим правилам.

Рассмотрим группу преподавателей. Дынные критериев сформированности приведены в схеме 1.


Схема 1

На схеме наглядно видно, что уровень сформированности компетенций у группы профессорско-преподавательского состава изначально был довольно высоким. Группа респондентов набрала 8 баллов, при этом ни разу не получив оценки «0», которая в свою очередь означала бы серьёзную уязвимость. Как мы отмечали при анализе ответов «проблемными» являются компетенции, связанные с новыми возникающими угрозами, а также с некоторыми практическими аспектами.

Следующими рассмотрим сотрудников административно-хозяйственного и учебно-вспомогательного персонала. Данные критериев сформированности приведены в схеме 2.


Схема 2

Анализируя уровень сформированности компетенций группы сотрудников, можно отметить, что он выше среднего. Сотрудники этой группы не допустили ошибок, которые могли повлечь за собой реализацию угроз безопасности. Самыми «проблемными» вопросами стали организационная защита информации, а также новые угрозы безопасности. Из 12 макисмально возможных баллов группа административно-хозяйственный и учебно-вспомогательного персонала набрала 8 баллов.

Третьей идёт группа руководящего состава, Данные критериев сформированности приведены в схеме 2.


Схема 3.

Схема наглядно показывает, что на первоначальном опросе группы руководящего состава уровень сформированности их компетенций был довольно низким. Этому свидетельствуют критерии оценки в «0» баллов, а также общий уровень ниже, чем у двух других групп. Данный результат обуславливается ещё и недостаточно серьёзным подходом к опросу и проблемам информационной безопасности в целом.

Как мы говорили ранее, все эти данные были учтены при разработке и наполнения курса занятий со всеми тремя категориями сотрудников. После проведения этих курсов было проведено повторное тестирование. Подведём его результаты также, в виде трёх схем.

Посмотрим на схемы групп профессорско-преподавательского состава (схема 4), административно-хозяйственного и учебно-вспомогательного персонала (схема 5) и руководящего состава (схема 6).


Критерий 1-Знание общих принципов функционирования системы защиты информации
Критерий 2-Знание основных регламентирующих документов
Критерий 3-Знание антивирусных программ, умение применять их
Критерий 4-Знание принципов функционирования программной части средств защиты информации
Критерий 5-Знание правил регистрации и использования машинных носителей информации в организации
Критерий 6- Знания в области новых угроз (в сети Интернет)

Схема 4.


Критерий 1-Знание общих принципов функционирования системы защиты информации
Критерий 2-Знание основных регламентирующих документов
Критерий 3-Знание антивирусных программ, умение применять их
Критерий 4-Знание принципов функционирования программной части средств защиты информации
Критерий 5-Знание правил регистрации и использования машинных носителей информации в организации
Критерий 6- Знания в области новых угроз (в сети Интернет)

Схема 5.

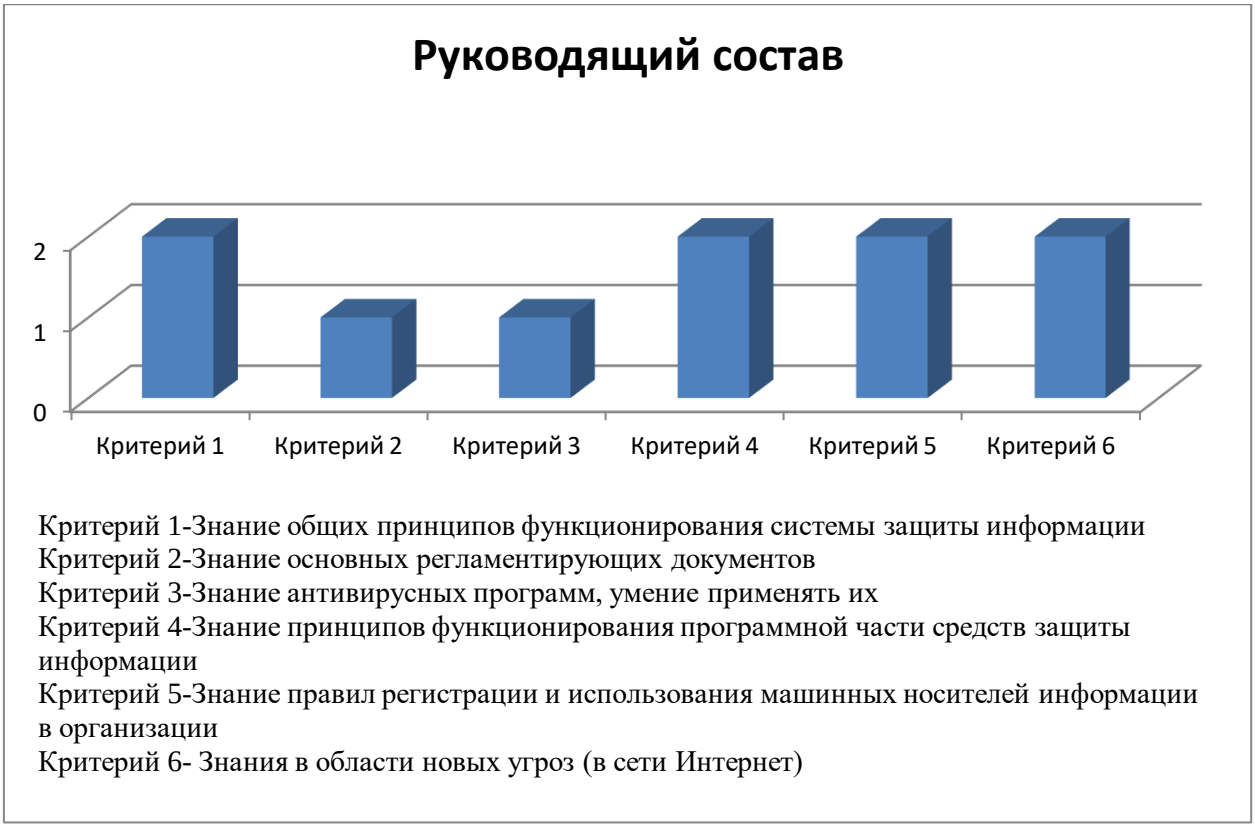


Схема 6.

*Подводя итоги* параграфа и опираясь на результаты повторного анкетирования всех участников эксперимента можно сказать, что уровень компетентности повысился. Если при первичном, «нулевом срезе» группы показывали результат в 6-8 баллов из 12 максимальных, то после проведенного курса лекционных и практических занятий уровень знаний и умений в области информационной безопасности стремится к максимуму и составляет 10-11 баллов из 12. Также стоит отметить тот факт, что все критерии, по которым были спланированы и проведены занятия в группах на повторном анкетировании составили 2 балла из 2 возможных.

## 2.4 Заключение

Подытоживая нашу работу по анализу формирования компетентности в области информационной безопасности сотрудников образовательной организации отметим, что проведена была большая работа по изучению научных источников по данной теме. Был описан понятийный аппарат по теме компетентностного подхода, даны определения основным терминам.

Далее была рассмотрена компетентность именно в информационной безопасности, для чего были проанализированы федеральные государственные образовательные стандарты для подготовки будущих педагогов. Также, были рассмотрены все основные нормативно правовые акты, регламентирующие вопросы информационной безопасности, а также основные типы сетевых атак. Опираясь на предыдущие выводы, а также требования ФГОС и иных нормативных документов был проведён анализ сотрудников образовательной организации, выделены 3 разных группы сотрудников, с каждой из которых будет проводиться отдельная работа, с учётом характерных особенностей. Проведён анализ федерального закона «Об образовании», выявлены сроки, в которые должно проводиться дополнительное обучение всех сотрудников. На основании этих выводов выдвинуты гипотезы:

- программу повышения квалификации необходимо проводить с учётом группы сотрудников, к которой относится конкретный сотрудник;
- дополнительное обучение необходимо проводить чаще, чем раз в 3 года, как это позволяет делать федеральный закон «Об образовании»;
- перед началом курса занятий необходимо провести опрос групп сотрудников, с целью понять какие компетенции сформированы хуже и учесть эти результаты в курсе.

В практической части нашей работы мы, опираясь на выводы сделанные ранее, приступили к проверке гипотез. Был проведён анализ образовательной организации, на базе которой проводилось исследование, выбраны структурные подразделения, в составе которых были сотрудники всех рассмотренных нами категорий. Изначально была проведена констатирующая часть педагогического эксперимента, а именно «нулевой срез», с использованием специально разработанного опросника, который показал уровень сформированности компетенций. После тщательного анализа всех ответов на опросник был подведён промежуточный итог

эксперимента, который показал сильные и слабые стороны в знаниях в области информационной безопасности у каждой из групп сотрудников.

Опираясь на результаты констатирующей части педагогического эксперимента было принято решение по внедрению методик формирования компетенций, а именно разработан план лекционных и практических занятий для каждой из групп сотрудников. Для этого были разработаны план-конспекты занятий, по которым, в течение 2 недель с группами сотрудников проводились занятия. По итогам курса практических и лекционных занятий, было проведено повторное тестирование, с целью оценить изменение в уровне сформированности компетенций у групп сотрудников образовательной организации. Помимо повторного тестирования, при анализе учитывались также вопросы обучаемых при проведении занятий.

После проведения курса лекций, был проведен анализ эффективности курса с помощью разработанной нами таблицы с критериями сформированности компетентности.

В процессе работы нами активно использовались мультимедийные технологии (в лекционных, и особенно – на практических занятиях), а также средства автоматизированного сбора данных, такие как Google формы.

Оценивая педагогический эксперимент, мы можем прийти к выводу, что он был удачным. Если при первичном, «нулевом срезе» группы показывали результат в 6-8 баллов из 12 максимальных, то после проведенного курса лекционных и практических занятий уровень знаний и умений в области информационной безопасности стремится к максимуму и составляет 10-11 баллов из 12. Также стоит отметить тот факт, что все критерии, по которым были спланированы и проведены занятия в группах на повторном анкетировании составили 2 балла из 2 возможных. Помимо этого, у всех групп повысилось понимание реальности реализации угроз информационной безопасности, а также улучшились практические навыки для противодействия им. Главной составляющей этого успеха мы считаем то, как был построен курс, а именно индивидуальный подход к каждой из групп

обучаемых, знание сильных и слабых сторон при формировании курса занятий.

При внедрения подобного подхода к формированию компетенций и в других организациях, стоит помнить об основных факторах, таких как:

- разделение сотрудников на группы, в которых компетентность в области информационной безопасности может быть различной;
- проведение «входного» тестирования, показывающего уровень сформированности компетенций каждой из групп обучаемых;
- составление курса практических и лекционных занятий в соответствии с полученными результатами тестирования.

При внедрении данного метода формирования компетентности было целесообразным внести изменение в практическую часть нашего эксперимента, а именно:

- увеличить количество вопросов в опроснике, до 20
- включить в опросник вопросы из всех частей в области информационной безопасности
- сделать вопросы с выбором ответов для упрощения их автоматической обработки.

Данные изменения призваны достигнуть большей автоматизации процесса при проведении таких курсов и как результат за меньшее время охватить большее количество сотрудников.

На наш взгляд практические наработки, полученные нами в ходе работы имеют большую перспективу применения, так как на проведение подобного курса не требуется большого количества ресурсов и времени, в то время как сам курс очень точечно может повысить самые «проблемные» места в компетенциях сотрудников в области информационной безопасности.

Анализируя результаты экспериментальной работы можно прийти к выводу о том, что комплексно был разобран вопрос формирования профессиональной компетентности в области информационной безопасности у сотрудников профессионального образования, сформирована методика их

формирования, готовая к внедрению в других образовательных организациях.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ


1. Albrechtsen E. A qualitative study of users' view on information security //Computers & security. – 2007. – Т. 26. – №. 4. – С. 276-289.
2. Peltier T. R. Information security fundamentals. – CRC press, 2013.
3. Salomon D. Data privacy and security. – Springer Science & Business Media, 2012.
4. Stallings W. et al. Computer security: principles and practice. – Upper Saddle River, NJ, USA : Pearson Education, 2012. – С. 978-0.
5. Thaw D. B. Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets : дис. – UC Berkeley, 2011.
6. Амелин Р. В. Информационная безопасность //Учебник. М. – 2010.
7. Андреева Г. М. Социальная психология. М.: Аспект Пресс, 2004. 415 с. Зимняя ИА Ключевые компетенции-новая парадигма результата образования //Высшее образование сегодня. – 2003. – №. 5. – С. 34-42.
8. Архангельский С. И., Михеев В. И., Машников С. А. О моделировании и методике обработки данных педагогического эксперимента:(Материалы лекций, прочитанных в Политехническом музее на факультете программированного обучения). – Знание, 1974.
9. Асмолов А. Г. Системнодеятельностный подход к разработке стандартов нового поколения //Педагогика. – 2009. – №. 4. – С. 18-22.
10. Афанасьев В. Г. Общество: системность, познание и управление. – Изд-во полит. лит-ры, 1981.
11. Байденко В. Компетенции в профессиональном образовании (к освоению компетентностного подхода) //Высшее образование в России. – 2004. – №. 11.

12. Батурин Ю. М., Морозов А. А. Структура и содержание магистерской программы≪ Информационное право и противодействие компьютерным угрозам≫ в МГУ им. МВ Ломоносова //Информационное право. – 2015. – №. 2. – С. 29-32.

13. Белов Е. Б., Лось В. П. О формировании компетенции «обладание культурой информационной безопасности» //Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. Самара: Инсома-Пресс. – 2017. – С. 60-63.

14. Беспалько В. П. Слагаемые педагогической технологии. – 1989.

15. Блауберг И. В., Юдин Э. Г. и сущность системного подхода. – М, 1973.

16. Бодалев А. А. и др. ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ КАК РЕЗУЛЬТАТ ОБУЧЕНИЯ В СРЕДНЕМ ПРОФЕССИОНАЛЬНОМ УЧЕБНОМ ЗАВЕДЕНИИ //ТРОИЦКИЙ ВЕСТНИК. – 2008. – С. 86.

17. Бондаревская Е. В. Личностно-ориентированный подход как технология модернизации образования //Методист. – 2003. – №. 2. – С. 2.

18. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников. — Текст : непосредственный // Современные тенденции технических наук : материалы I Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа : Лето, 2011. — С. 8-13. — URL: https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 25.10.2020).

19. Бояров Е. Н. Концептуальные подходы к обучению специалиста информационной безопасности в университете //СПб.: РГПУ им. АИ Герцена. – 2008.

20. Буланова-Топоркова М. В. Педагогические технологии: учебное пособие для педагог. спец //М.: Ростов н/Д: Март. – 2006.

21. Вербицкий А. А. Контекстно-компетентностный подход к модернизации образования //Высшее образование в России. – 2010. – №. 5.

22. Вербицкий А. А., Ильязова М. Д. Формирование инвариантов компетентности студента: ситуационно-контестный подход //Высшее образование сегодня. – 2011. – №. 3. – С. 34-38.

23. Выготский Л. С. Системно-деятельностный подход в практике работы специалистов с обучающимися с ОВЗ //Молодой ученый. – 2019. – Т. 11. – С. 260.

24. Галатенко В. А. Основы информационной безопасности. – 2008.

25. Галатенко В. А. Основы информационной безопасности. – 2008.

26. Гальперин П. Я. Опыт изучения формирования умственных действий //Вестник Московского университета. Серия 14. Психология. – 2017. – №. 4.

27. Генике Е. А. Профессиональная компетентность педагога. – 2008.

28. Горбатов В. С., Кондратьева Т. А. Правовые основы информационной безопасности: Учеб. пособие. – 1998.

29. Городов О. А. Информационное право. – 2016.

30. Даньков А. П., Максименко В. Н. Предпосылки появления новых уязвимостей и угроз информационной безопасности в сетях сотовой связи //Мобильные системы. – 2005. – №. 1. – С. 38-40.

31. Доктрина информационной безопасности РФ (утв. Президентом РФ 09.09.2000 г. № Пр-1895) – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ Дата обращения 23.01.2021 г.

32. Доронин А. С. Разработка мероприятий по обеспечению информационной безопасности в структурном подразделении вуза (на примере высшей школы Санкт-Петербургского политехнического университета Петра Великого): выпускная квалификационная работа бакалавра: 20.03. 01-Техносферная безопасность; 20.03. 01_02-Безопасность технологических процессов и производств. – 2018.

33. Дремлюга Р. И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ

законодательства США и России //Журнал зарубежного законодательства и сравнительного правоведения. – 2018. – №. 6 (73).

34. Журавлев Ю. А. Правовые основы обеспечения информационной безопасности юридических лиц : дис. – 2009.

35. Журин А. А. Информационная безопасность как педагогическая проблема //Педагогика. – 2001. – №. 4. – С. 48-55.

36. Занина Л. В., Меньшикова Н. П. Основы педагогического мастерства //Ростов н/Д: Феникс. – 2003. – Т. 124.

37. Зеер Э. Ф. Модернизация профессионального образования: компетентностный подход //Образование и наука. – 2004. – №. 3.

38. Зефиров С. Л., Алексеев В. М. Способы оценки информационной безопасности организации //Труды Международного симпозиума «Надежность и качество». – 2011. – Т. 2.

39. Зимняя И. А. Ключевые компетенции–новая парадигма результата образования //Эксперимент и инновации в школе. – 2009. – №. 2.

40. Иванов Д. А. Компетенции и компетентный подход в образовании //Школьные технологии. – 2007. – №. 6. – С. 77-83.

41. Иванов Д. А. Компетенции и компетентный подход в образовании //Школьные технологии. – 2007. – №. 6. – С. 77-83.

42. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. – 2019.

43. Коваленко А. П., Белов Е. Б. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) //Научные и методологические проблемы информационной безопасности/под ред. ВП Шерстюка.–М.: МЦНМО. – 2004.

44. Коваленко, А. П., Белов Е. Б. Концепция подготовки кадров в области обеспечения информационной безопасности (проблемы, анализ, подходы) //Научные и методологические проблемы информационной безопасности/под ред. ВП Шерстюка.–М.: МЦНМО. – 2004.

45. Козырев Н. А., Козырева О. А. Педагогическое моделирование как продукт и метод научно-педагогического исследования //Современная педагогика. – 2015. – №. 8. – С. 14-23.

46. Корнюшин П. Н., Костерин С. С. Информационная безопасность //Владивосток: ТИДОТ ДВГУ. – 2003. – С. 154.

47. Корнюшин П. Н., Костерин С. С. Информационная безопасность //Владивосток: ТИДОТ ДВГУ. – 2003. – Т. 154.

48. Коробеев А. И., Дремлюга Р. И., Кучина Я. О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации //Всероссийский криминологический журнал. – 2019. – Т. 13. – №. 3.

49. Краевский В. В. Методология педагогического исследования. – 1994.

50. Круглов А. А., Скородумов Б. И. Информационная безопасность: от угроз к рискам //Информационное противодействие угрозам терроризма. – 2007. – №. 6. – С. 99-108.

51. Крылов Г. О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации //URL: http://www. law. edu. ru. – 2007.

52. Крысин А. В. Информационная безопасность. Практическое руководство //М.: СПАРРК. – 2003.

53. Кузьмина Н. М., Толстякова О. В. Формирование организационной стратегии управления кадровым потенциалом: компетентностный подход. – 2015.

54. Кун Т. Структура научных революций. – Рипол Классик, 1975.

55. Лаврентьев Г. В., Лаврентьева Н. Б. Методика оценки педагогической деятельности преподавателя высшей школы в процессе внедрения новых технологий обучения //Барнаул: Изд-во АГУ. – 2000.

56. Лаврентьев Г. В., Лаврентьева Н. Б. Педагогическая компетентность преподавателя как условие внедрения инновационных технологий Текст //Вестник алтайской науки. – 2000. – №. 1. – С. 137-144.

57. Лакатос И. Фальсификация и методология научно-исследовательских программ. – 1995.

58. Леонтьев А. Н. Проблема деятельности в истории советской психологии //Вопросы психологии. – 1986. – №. 4. – С. 109-120.

59. Львов Л. В. Роль умений в достижении профессиональной компетентности будущих специалистов //Образование и наука. – 2004. – №. 5.

60. Марков А. А. Некоторые аспекты информационной безопасности в контексте национальной безопасности //Вестник Санкт-Петербургского университета. Социология. – 2011. – №. 1.

61. Мельников В. П. Информационная безопасность и защита информации: доп УМО для вузов //М.: ИЦ Академия. – 2011.

62. Мещеряков Р. В., Шелупанов А. А. Комплексное обеспечение информационной безопасности автоматизированных систем. – 2007.

63. Нагайченко Н. Н. Критериальная основа мониторинга воспитывающей среды образовательного учреждения //Ярославский педагогический вестник. – 2011. – Т. 2. – №. 4.

64. Петровский А. В. Личность в психологии с позиций системного подхода //Вопросы психологии. – 1981. – Т. 1. – С. 57.

65. Полани М. Личностное знание. – Рипол Классик, 1985.

66. Поляков В. П. Аспекты информационной безопасности в информационной подготовке. – 2016.

67. Полякова Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России. – 2008.

68. Поппер К. Логика и рост научного знания. – М, 1983. – Т. 548.

69. Приказ Минздравсоцразвития России от 11.01.2011 № 1н – Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_97378/6a5000401d4e1ae92043c3f29ee85544be486b52/ Дата обращения:23.01.2021 г.

70. Равен Д. Компетентность в современном обществе. Выявление, развитие и реализация. – 2002.

71. Семененко В. А. Информационная безопасность. – МГИУ, 2010.

72. Сластенин В. А. Субъектно-деятельностный подход в общем и профессиональном образовании //Сибирский педагогический журнал. – 2006. – №. 5.

73. Талызина Н. Ф. Деятельностный подход к механизмам обобщения //Вопросы психологии. – 2001. – №. 3. – С. 3-16.

74. Танова Э. В. Формирование компетентности в области защиты информации у школьников в процессе обучения информатике : дис. – 2005.

75. Уголовный кодекс Российской Федерации, глава 28 – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/ Дата обращения 23.01.2021 г.

76. Уфимцев Ю. С. Информационная безопасность России. – 2003.

77. Федельный закон "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_140174/168256bdcb9538e86c8375f663d57802eac03dcf/ Дата обращения:23.01.2021 г.

78. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 44.03.01 Педагогическое образование – Режим доступа: http://fgosvo.ru/uploadfiles/fgosvob/440301.pdf Дата обращения:23.01.2021 г.

79. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 050100 Педагогическое образование (квалификация (степень) бакалавр) – Режим доступа: https://narfu.ru/upload/iblock/f26/fgos_050100.pdf Дата обращения 23.01.2021г.

80. Федеральный закон "О статусе военнослужащих" от 27.05.1998 N 76-ФЗ URL:http://www.consultant.ru/document/cons_doc_LAW_18853/Дата обращения -23.01.2021г.

81. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/ Дата обращения 23.01.2021 г.

82. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ Дата обращения 23.01.2021 г.

83. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

84. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/ Дата обращения 23.01.2021 г.

85. Фейрабенд П. Против метода. Очерк анархистской теории знания. – 1986.

86. Хуторской А. В. Ключевые компетенции как компонент личностно-ориентированной парадигмы образования //Народное образование. – 2003. – №. 2. – С. 58-64.

87. Цирлов В. Л. Основы информационной безопасности автоматизированных систем //М.: Феникс. – 2008. – С. 173.

88. Шерстюк, В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности //Информационное общество. – 1999. – №. 5. – С. 3-5.

89. Щербакова В. В. К вопросу о профессиональной компетентности //Сибирский педагогический журнал. – 2008. – №. 2.

90. Якиманская И. С. Технология личностно-ориентированного образования. – 2000.

91. Ясенев В. Н. Информационная безопасность в экономических системах: Учебное пособие //Новгород: Изд-во ННГУ. – 2006. – Т. 253.

92. Ясенев В. Н. Конспект лекций по информационной безопасности.